Induction Policy for New Trustees

DATE: 31 August 2021
REVIEW DATE :   7 December 2023
NEXT REVIEW DATE: 7 December 2026

Contents

The Board of Trustees and Chief Executive Officer (CEO) believe it is essential that all new Trustees receive a comprehensive induction package covering a broad range of issues and topics. There is a commitment to ensure that the new Trustees are given the necessary information and support to fulfil their role with confidence. The process is seen as an investment, leading to more effective governance and retention of Trustees.

Purpose

- To welcome new Trustees to the Board and enable them to meet other members.

- To facilitate a quick engagement with the workings of the Board.

- To encourage a shared responsibility and an equitable contribution to the workload of the Board.

- To encourage new Trustees to visit the schools to experience their atmosphere and understand their ethos.

- To meet the Headteachers, staff and students.

- To explain the partnership between the CEO, Local Governing Body (LGB), Executive Team and Board of Trustees.

- To explain the role and responsibilities of Trustees.

- To give background material on the schools and current issues.

- To allow new Trustees to ask questions about their role and/or the Trust.

- To explain how the Board, LGBs and committees work.

- To allow new Trustees to join the committee(s) of their choice.

New Trustees as soon as is practicable will:

- Be welcomed to the Board by the Chair.

- Be invited by the CEO to visit the schools.

- Have the opportunity to tour the schools and meet staff and students.

- Receive an informal briefing on the Trust from the CEO and/or Chair.

- Be asked to complete a DBS check, register of interests and other documentation as required.

- Be required to undertake UK GDPR training (30 minute video – appendix 3).

- Be required to undertake Cyber Security Training (30 minute video – appendix 4)

- Be asked to sign a Code of Conduct.

- Be asked to register for Governor Hub (see below).

New Trustees will receive within two weeks of appointment:

- The DfE Governance Handbook

- The Trust's Code of Conduct

- The DfE's "Keeping Children Safe in Education"

- The DfE's "Competency Framework for Governance"

- The ESFA's "Academies Financial Handbook

- An outline of any training Trustees are required to attend

- Minutes of the last Board meeting and the details of any committees including terms of reference

- The Trust Scheme of Delegation.

- Dates for future Trustees' meetings

- Details of how to contact the other Trustees

- Policy documents relevant to committee membership

- Details of how to contact the Trust including the e-mail address and website

- A calendar of events.

Areas of discussion, which the Chair of Trustees will cover with the new Trustee, should include:

- Background to the Trust

- Current issues facing the Trust

- Visiting the Trust

- The relationship between the CEO, Local Governing Bodies (LGB), Executive Team and Board of Trustees

- An overview of the Trustee's role including confidentiality

- How the Board meetings are conducted including the use of the Governance portal

- Child Protection arrangements for the Trust and the Trustee's role in safeguarding these

- How to propose agenda items

- Importance of giving apologies if unable to attend meetings

- Trustee training

Onboarding and Induction Process: Step by Step

1. The Governance Professional to the Board will contact you in the first instance with your appointment letter and this onboarding pack. They will ask you to bring in identification (passport/driving license and proof of address).

2. DBS – an email will be generated and sent to you from an external system once a new DBS application is created, unless you are already a member of the DBS update system. Please follow the instructions on the email to complete your DBS application.

3. Once your DBS check is complete, the admin lead will contact you to provide/request the following:

- ID photo for your ID badge
- OAK IT set up
- Information about the Governor Hub system
- Training Resources: NGA membership (including the Learning Link), the Key and the Leicestershire Governor Development Service. See Appendix 2.
- You will be sent a link to statutory Safeguarding Training

4. The CEO of the Trust will arrange to meet with you and you will have the opportunity to visit the schools with him.

Governor Hub

Governor Hub is an online storage platform and tool that's designed specifically for governing boards where we share agendas and associated documents, news, training options and other communication. You will be registered for Governor Hub once your new IT account (see below) is set up.

Declaration of Interests

The Board of Trustees and individuals at all levels of Trust governance have a responsibility to act impartially and avoid any conflict between their business and personal interests and those of the individual academy and Trust as a whole. There is a legal duty on all those involved in Trust governance to declare an interest likely to lead to questions of bias when considering any item of business at a meeting and for the individual concerned to withdraw, if necessary, whilst the matter is considered.

To help put this duty into practice, the Trust is required to establish and maintain a register of interests. This should include, if appropriate, the company by whom Trustees, Members, local governors etc. are employed and directorships, significant shareholdings or other appointments of influence within a business or other organisation which may have dealings

with the academy or Trust. When completing the declaration of interests form you should include your own interest and those of any member of your immediate family (including partners) or other individuals known to you who may exert influence. This form should be completed on commencement of your role within the Trust and updated on an annual basis.

The forms are completed on Governor Hub under the 'Declarations and Confirmations' section which can be accessed by clicking your profile and navigating to the relevant tab:

About You   Declarations & Confirmations   Training   Settings

Under this tab, you will also confirm you agree to abide by the Code of Conduct, and that you have read the KCSIE (Keeping Children Safe in Education) document. It is essential you complete these declarations.

Under the Training Tab, you will be able to record the GDPR Training (appendix 2) and Cyber Security Training (appendix 3).

In the Documents area of Governor Hub you will find an Induction for Trustees folder, which contains relevant information and guidance to start you on your journey.

IT Set Up

To comply with GDPR we provide all our Trustees with an OAK IT account. Your OAK email will be our primary mode of communication with you. Calendar invites for all Trust Board and Committee meetings will be sent to your OAK email address and we will share meeting agendas and supporting documentation via Governor Hub, on which your new email will be registered.

- In your web browser type in outlook.office365.com
- When prompted, enter in your OAK email
- When prompted again, enter your password
- You will be now logged into your OAK email account
- If you have an issues with your OAK account, please submit a ticket to the helpdesk: helpdesk@aitn.co.uk

Statement of review

The Board of Trustees has agreed that this policy will be reviewed on a three yearly basis unless Government guidance or legislation forces an earlier revision. Any review will take into consideration all aspects of applicable legislation and advice current at the time of the review.

Appendix 1: New Trustee Checklist

Induction Procedure	Initial when complete
Welcome	
Welcome to the Board by the Chair	
Invited by the CEO/Chair to visit the academies	
Toured the academies and met staff and students	
Explanation of statutory responsibilities	
Forms for completion	
Completed identification process for DBS check	
Register with Governor Hub	
Completed Trustee Profile/Contact Details form/ on Hub	
DfE Keeping Children Safe in Education – confirmation read Part 1 & 2	
Details of National Governance Association (NGA) login	
Trustee Code of Conduct	
Watch UK GDPR Training Video (*Appendix 3)	
Record UK GDPR training on Hub	
For information/reading	
Latest Ofsted reports	
Vision and Values of the Trust/background to academies	
Scheme of Delegation	
DfE Governance Handbook	
Trust Business Continuity Plan	
DfE Competency Framework for governance	
ESFA Academies Financial Handbook	
Trust Accounts	
Articles of Association	
Minutes of the last Board meeting	
Dates of future Trustees' meetings	
Contact details of Trust and other Trustees	
Policy documents relevant to committee membership and other relevant policies	
Risk Register	
Privacy Notice	
Organisation chart/staff list	
Calendar of events	

Appendix 2: Training opportunities

Where can I access training as a Governor / Trustee?

See below for sites specialising in specific training (safeguarding, SEN, Curriculum, Pupil Premium, and much more) and more generic governance training:

- Governor Hub / including Governor Hub Knowledge

[GovernorHub Knowledge (thekeysupport.com)](#)
You will receive a registration link to Governor Hub once you become a governor. Your clerk will explain this as part of induction. Governor Hub is linked with the Key (see Knowledge tab) and this is a wealth of information including [training courses](#) and [learning pathways](#). They have some good induction bitesize courses for governors and trustees too. This training is recorded on Governor Hub when complete.
- Leicestershire Governor Development Service – all schools are members

[Leicestershire Traded Services](#) – log in and go to 'resources' tab for full training schedule
You should have been added to this when you joined as a governor; if you do not have access, please let your clerk know. You can also sign-up here: [New Account Request | Leicestershire Traded Services](#). Full brochure and guide on how to use the service are on Governor Hub in the training folder.
- NGA / Learning Link

As part of the LTS (above), schools and trustees also have access to the Learning Link: [Learning Link e-learning for school governors and trustees | National Governance Association (nga.org.uk)](#) with many excellent resources for specific and general areas of governance. You will need to register: [Registration - Enable (vc-enable.co.uk)](#) and choose your school (Trustees should choose Manor High). Once the NGA have confirmed, you will be able to log in. Any problems, let your clerk know.

Other sites
- Governors for schools – includes webinars, e-learning and news. Free.

[Online training and support for governors - Governors for Schools](#)
- CST (for Trustees)

[Login (cstuk.org.uk)](#)
The trust is a member; please contact the central team for the membership number to access courses specific to being a trustee in a MAT.

Introduction and Induction webinars:

[The first 100 days as a trustee - Governors for Schools](#)
[Induction for academy governors on local governing bodies | GovernorHub Knowledge (thekeysupport.com)](#)
[Induction for academy trustees | GovernorHub Knowledge (thekeysupport.com)](#)
[Welcome to Governance](#)
[Induction Training for new Governors](#)

Introduction to Governance webinar: [Introduction to governance webinar - Governors for Schools](#)
A free webinar to direct colleagues/friends/family/acquaintances to if they wish to find out more about the role.

If you know of anyone who would like to become a Trustee, or find out more about the role, this is a useful page to direct them to: [Academy trustees: who are they and what do they do?](#)

(governorsforschools.org.uk)

For succession planning or Chair development

Various courses including:
Leading Governance Development for Chairs | National Governance Association (nga.org.uk)
Learning Link Succession Planning
LTS Chairs' Forum
The Crucial Role of the Chair

If your LGB feels there is a bespoke need for particular training, then please let the central team know admin@oaktrust.org and we can organise this for you.

Appendix 3: UK GDPR Training

Training video

UK GDPR compliance requires the engagement and involvement of all school staff, LGBs and Trustees.

Ensuring that staff are aware what UK GDPR is, how it impacts on maintaining role, remaining vigilant and understanding their personal responsibility and obligations is essential. Training staff, governors and volunteers is recommended by our DPO to be undertaken on an annual basis.

The training provided by our DPO has been updated to provide a focus for the school workforce, including volunteers, and for trustees and governors. Each training is around 30 minutes, and the individual links can be shared or used for training at meetings, briefings, or inset days. It is vital that LGBs and Trustees are aware of the ongoing GDPR processes.

Keeping a record of attendees and ensuring that new staff, volunteers, governors, and trustees watch the videos and read the associated guides is a matter for each school or trust to arrange as part of the existing CPD monitoring process. For LGBs and Trustees, we ask that clerks plan for this training to be included in the agenda for the Autumn meeting on an annual basis.

The training video to be included is here:

UK GDPR training video Governors and Trustees

https://vimeo.com/742641497/5e2eb7bb3f

Appendix 3(i): UK GDPR Overview for Governors and Trustees

Data Protection –The Responsibilities of the Data Controller

Introduction

25 May 2018 saw the implementation of the General Data Protection Regulation (GDPR) and the implementation of the Data Protection Act 2018 (DPA). This was a reform of the previous Data Protection Act 1998. So much had changed that new legislation was required to provide more updated protections for individuals and a framework to manage technological developments.

School are classed a public authorities and have additional obligations, principally to appoint a suitable Data Protection Officer. Everyone in the school community needs to understand their obligations, responsibilities and rights.

This is an overview of key issues and concepts for schools and academies. It looks at what needs to happen, and gives an overview of who is who in this very jargon heavy world.

Following the media hysteria about GDPR, everything suddenly died away. However, the legal obligations that GDPR and the DPA place on schools has not changed. The ICO has begun to audit schools, there have been huge fines for some companies, BA and the ICO officers are taking a more forensic approach to complaints. GDPR compliance is also forming part of some internal audits, Ofsted inspectors asked for details on one occasion and some external auditors have queried compliance for annual reports.

Being on top of GDPR is an essential part of school management.

What is the GDPR?

This is a European Directive that is now part of the UK domestic legislation. Brexit will not change it.

What is the point of the GDPR?

The GDPR and new DPA exist to protect individuals' data. It is a series of safeguards for each of us. It is regulation designed to protect you, me and our families. In schools we handle data about children and adults every day. Some of that is very simple, a child's name on a book. Other information is far more sensitive, an EHCP for a child or an Occupational Health report for an adult for example.

Making sure that personal data is properly looked after is the whole point of the GDPR.

If it is shared without my permission or a legitimate purpose it could cause embarrassment, financial loss or have some other direct impact. If the data held is wrong or inaccurate it is important it is put right.

However, GDPR was never designed with schools in mind. The focus is on big business, international brands, banking and insurance sectors and government. The GDPR exists to protect individual rights in an increasingly digital world, and schools are caught up in this.

Who does it apply to?

Everyone, including schools. As Public Bodies schools have more obligations than some small businesses. It is mandatory to comply with the GDPR and proposed provisions in the new Act.

Do schools have to change all of their policies and procedures?

Schools are good at data protection, it is simply part of day to day school life. However, GDPR requires some reviews to be in place, it is necessary to take stock of what data is held. Being clear about what is collected, why it is collected, how it is used, stored and disposed of is at the core of good GDPR compliance.

Relations with those who process data on behalf of the controller should be GDPR compliant. New processes will need to be subject to a greater degree of scrutiny, a Data Privacy Impact Assessment.

Doing this will assist in compliance with the key principles.

What are the 6 key principles of the GDPR?

Lawfulness, transparency and fairness.

School's must have a legitimate reason to hold the data, and need to tell people what data school collects and how it is used.

Collect data for a specific purpose and use it for that purpose

So, data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy.

Retention

There must be a policy that requires data to be stored for limited periods of time about individuals. You should not store data for longer than you need it, or for historical archive reasons.

Security

Ensuring that physical, cloud and other electronic storage of data is secure is vitally important. Everyone has a responsibility for the data they hold and process. This also includes third party contractors.

What is Data?
Any information that relates to a living person that identifies them. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions.
Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.
Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Who is a 'Data Subject'?

Someone whose details we keep on file. Some details are more sensitive than others. The GDPR sets out which collection of details such as health conditions and ethnicity are more sensitive than names and phone numbers.

Essentially the whole of Data Protection exists to make sure that information held

about us is treated with proper care and respect.

Data Subjects' Rights

Schools must inform people about how they hold data, and also that individuals have a right to access it. This can be limited in some instances where child protection is involved, or if there are legal or contractual exemptions. Schools need to tell people how they can do this and explain the complaints policy.

If data is inaccurate, no longer needed or old and serves no purpose the data subject has a right to have the data amended or deleted.

Children's data is particularly sensitive, and children have a right to ask for certain data to be deleted – this really is linked to social media accounts but has implications for schools.

If there are pending or potential legal proceedings data must be preserved.

Who is a 'Data Controller'?

The organisation that is ultimately responsible for the data collected about the data subject. It will be the governing body or academy trust. It can also be the head depending on the school structure.

The Data Controller must be satisfied that suitable policies and procedures are in place.

The Data Controller must ensure that:-

Suitable Privacy Notices are in place
The Data Protection Policy is fit for purpose
In the event of a breach, suitable plans are in place to manage the breach and liaise with the Information Commissioner
There is awareness of the changes across the school workforce, and that staff understand their personal responsibilities and liabilities
The concept of 'Privacy by Design' or collecting only as much data is necessary for a task, is embedded in the school
A suitable Data Protection Officer is appointed
New processes are assessed using a Data Privacy Impact Assessment
Everyone can understand how their data is held, and how to request amendments or erasure is necessary
Enabling a Data Subject to complain is a simple procedure
Data is processed and categorised using one of the lawful criteria for processing

Whilst the Data Controller can delegate actions to their employees, responsibility sits with the Data Controller. In maintained schools it is the governing body, in academies it is the trust.

Article 5(2) states that
"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Who is a 'Data Processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected on behalf of the data controller. It can be a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the LA. Of course, staff in schools are processing data.

Data controllers must make sure that data processors are as careful about the data as the controller themselves. The GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

12 months is checking and confirming that these suppliers are compliant is important. Future supplies, or renewal of contracts, will need a DPIA in place.

Processing data

Schools must have a reason to process the data. The GDPR has 6 conditions for lawful processing, and processing must be within one of them to comply.

School has the consent of the Data Subject

It is necessary for the performance of a contract

It is necessary to comply with a legal obligation

It is required to protect the vital interests of the data subject, or another person

It is necessary for the performance of a task carried out in the public interest or the exercise of official authority

It is necessary for purposes of legitimate interests pursued by the controller or a third party (but not where the data subject's rights override the controller)

Sensitive Data

Processing sensitive data in schools requires careful consideration. Gaining consent is required, unless there is another legal basis to do so, for example safeguarding or protection of vital interests.

Data Protection Officer

Every public authority, which includes schools, must have a Data Protection Officer.

The data protection officer shall have at least the following tasks:

to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the GDPR

to monitor compliance with the GDPR and DPA

to provide advice where requested about the data protection impact assessment and monitor its performance

to cooperate with the supervisory authority and manage the breach procedure

to advise about training and CPD for the GDPR

should have expertise in national and European data protection laws and practices and an in depth understanding of the GDPR.

to support the rights of Data Subjects

The Data Protection Officer's details should be on the school website, Privacy Notices and in the Data Protection Policy.

Privacy by Design

The idea of the GDPR is that data should be carefully managed and curated. New processes should be subject to assessments. These are to consider risk and how this can be managed as part of the procurement process. This has an impact in classrooms and school offices.

Information Commissioner Office (ICO)

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations. The ICO has the power to issues fines, publish decisions and seek undertakings. The new Act proposes increases to the power ICO to fine, to bring prosecutions, order compensation and other sanctions.

Breaches

Breach preparation is key. Breaches happen as a result of human error. They are rarely deliberate (unless planned criminal activity) more likely to be as a result of forgetfulness or mistake. An email sent to the wrong person is the most frequent source of a breach.

The GDPR requires certain breaches to be notified to the ICO within 72 hours. In some cases 72 hours will not be long enough to complete the investigation. A key part of the response must be risk assessment of the data that has been lost and the planned remedial action to be taken as a consequence of the breach.

The Data Controller will need to have confidence that these can be handled, and reported back to the controller as necessary. Many breaches are internal action only, the more serious are reported to the ICO. Advice from the DPO is important to manage the process effectively.

Sanctions

New powers and sanctions apply – up to 20 million euros or 4% of global turnover in fines. Although no school has yet been given a financial penalty. It is now possible for individuals to seek compensation is new with the GDPR.

Criminal offences for reckless or deliberate breaches can affect every single one of us. The message must be that from a personal point of view the GDPR is that everyone who interacts with data is potentially culpable. Reckless loss of data can include leaving a file open for others to view it, it could be inadequate security measures. Reckless has a wide scope and the Data Controller has a responsibility to take measures, failure to do so could also be considered reckless.

Safeguarding

GDPR does not, at all, ever, prevent information sharing to protect children and/or vulnerable adults. Schools have statutory and other obligations to ensure that children are protected. Serious case reviews often point to the lack of good information sharing as a feature of child deaths.

Understanding that there is a process to be followed and mechanisms to ensure that

data is shared appropriately need to be in place.

If in doubt the matter should be referred to the Designated Safeguarding Lead, the DPO and the local authority protection teams.

What is required?
The guidance from the ICO is clear. Understand and know your data. Mapping is a tedious, time consuming but vital task. Schools must ensure that they understand their data and how it is to be collected, used, stored and destroyed. Without that knowledge there cannot be good GDPR compliance.
Every school has to have a Data Protection Policy that reflects the GDPR requirements. This will be on the website and will explain in more detail obligations and how the school will meet these.
Every school should have a person who is designated to be responsible for data protection compliance, and to have a Data Protection Officer (who may be within school or outsourced).

IT security is a key element of data protection and an acceptable use policy, IT policy or similar is likely to be in place also. Compliance is likely to be mandatory and will include things such as not using a personal email address, only using encrypted mobile devices and the process for locking a computer if away from the desk.

The more information on the website, the better.

IT and Information Security

Many processes used on a daily basis in schools use IT. Whether this is emails, progress tracking, attendance management, cashless payments or many, many more examples.

Making sure that the IT systems, levels of access and protective measures are suitable is the responsibility of the Data Controller, but in practice will be delegated to operational leads to check and secure the outcomes.

Checking firewalls, server security and the location of and protection of back ups will be important elements of this strategy.

The Data Controller must be satisfied that effective IT security is in place, that it is well managed and up to date.

Encryption
The Information Commissioner has issued a number of notices and guidance about how important encryption is –

'Encrypting data whilst it is being stored (eg on a laptop, mobile, USB or back-up media, databases and file servers) provides effective protection against unauthorised or unlawful processing. It is especially effective to protect data against unauthorised access if the device storing the encrypted data is lost or stolen.' ICO

If a laptop that is encrypted is stolen, the chance of a data breach will be minimal, if a laptop with a password is stolen the likelihood of a data breach is very high. Encryption can also be applied to tablets, ipads, smart phones and memory sticks. The Data Controller must be satisfied about how mobile devices are protected. What is the school policy about personal devices? How does that fit with good GDPR?

Email
Email is not a secure form of messaging. It has been said that an email has as much security as a postcard.

Sending sensitive data by email must be done in a secure way. That might include password protected word, excel or pdf documents. It might include getting parental consent to use email for more sensitive correspondence, or finding an alternative by sending an email with a securely controlled attachment.
Personal emails should not be used for school business, and that includes governors and trustees emails too. A Subject Access Request can be applied to personal accounts in some cases.

Staff, Parent's and Pupils Rights to view Data

Unless there is a reason to refuse that is linked to legal confidentiality, safeguarding the child or another person, a contractual or regulatory reason the basic position is that all data should be disclosed on request.

A 'Subject Access Request' (SAR) process should be in place. It should be clear and if any parents want information about their child, or themselves, that is more than the usual round of parent's evening and reports, then they should be directed to the process on the website. Any request made to you should be directed to the in school person responsible for dealing with a SAR.

Each request must be considered on a case by case basis.
The school must have a process to manage the request and the timeline to comply. The Data Controller is obliged to comply with the timeline, and be satisfied that those acting on its behalf have a clear understanding of what needs to be done.

Subject Access Requests have increased over the last 12 months. Some have been easy to manage, some have involved hundreds and thousands of emails. One has

been in excess of 100,000 emails. The resources to manage the scale of these requests can be very significant. Having a process to destroy emails, unless they are required, is very important.

Overview

All schools have sensitive data, and it is used in classrooms and in the office. When an individual uses, accesses, collects or edits that data they are responsible for ensuring the security of the data. Getting consent to use the data is a very important factor, but schools can share data with other professionals to safeguard children and help detect crime. Every time we are asked to share data we need to know what is the lawful basis for doing so, and if in doubt check, with a line manager or with a lawyer.

Keeping data safe is an obligation on the school and the individual. Schools must make sure they have suitable processes, effective policies and the right support for staff. Staff must make sure they understand their obligations and need to comply.

If there is ever a breach, then working together will be the best way to put it right, learn the lessons and move forward.

As the Data Controller, governing boards and trustees have a direct legal obligation to ensure that suitable polices, procedures and measures are in place.

What do schools need to do?

Preparing to be GDPR complaint requires schools to undertake several steps. Implementation is rapidly approaching and taking a planned, considered approach will enable compliance. Preparing for GDPR compliance will involve everyone in school to some degree. It cannot sit on one person's desk. Lead individuals need to be identified.

Across the school workforce it is likely that everyone will need to take a look at their own practice and workspace.

To give an overview and a sense of the scale of the task, this is a summary of what each school needs to consider.

Everything starts with a full Data Protection, which should include: -

- Data mapping – a record of data collected and how it is stored, used and retained

- Reasons for processing data – a system review to look at consent and the other reasons why school holds and processes data.

- Policy review - not a full-scale review of every policy, but checking polices that require school to share information with 3rd parties that this is GDPR compliant. It might be a simple as adding an extra line to refer to GDPR.

- Training & Awareness in the school community - all staff, volunteers, trustees and governors

- Third party contract review

- Staff contracts and HR compliance

- Development of Data Privacy Impact Assessments - Privacy by Design

- Appointment and remit of the Data Protection Officer

- Role and responsibility

- Breach preparation

- Devise and agree a suitable compliance timeline - with regular reviews and updates

Appendix 4 – Cyber Security Training

Cyber-attacks are no less frequent or less severe in education. In fact, they seem to be gaining ground in prevalence year on year as instances of breaches in schools and higher education are widely reported. Not only does this have the potential to affect the finances or running of the school, but can also impact the privacy of the pupils themselves and the school's reputation. Therefore, Cyber security is part of the wider DfE guidelines for IT security and training is required to adhere to insurance requirements.

OU IT support provider is responsible for securing our systems and ensuring basic protection from cyber-attacks. However, no technological solution is 100% effective. Often the best defence is staff who are aware of the main cyber risks and threats to a school. School staff can be a crucial part of a schools' cyber defences by following some key cyber security steps. As a result, it is vital that new staff undertake cyber security training at their earliest convenience. The training video can be viewed here: [Cyber security training for school staff - NCSC.GOV.UK](#)