multum in parvo

Windrush Valley School

Policy Documents Annual Review Record

Citation	This document shall be cited as: **Data Protection Policy** Associated policies: Staff Privacy Notice Privacy Notice for Parents and Pupils Staff Code of Conduct ICT Acceptable Use Policy Remote Working: Mobile Device Policy Data Asset management and Retention Policy Safeguarding Policy
Regulatory standard	Part 1: Quality of Education Provided
Person responsible	Headteacher
Comments to	Headteacher
Last reviewed/updated	July 2020
To be reviewed/updated	July 2022
Reason for review/update	Regular review cycle
Person reviewing/updating	Victoria Barron
Source/author	Alan Wood
Implementation	Immediate and on-going

multum in parvo

DATA PROTECTION POLICY

1. Background

Data protection is an important legal compliance issue for Windrush Valley School Limited. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the School's privacy notices). The School, as "data controller", is liable for the actions of its staff, proprietor and governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

The law changed on 25 May 2018 with the implementation of the General Data Protection Regulation (**GDPR**) – an EU Regulation that is directly effective in the UK, regardless of Brexit status – and a new Data Protection Act 2018 (DPA 2018) was also passed to deal with certain issues left for national law. The DPA 2018 included specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Without fundamentally changing the principles of data protection law, and while providing some helpful new grounds for processing certain types of personal data, in most ways this new law has strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (**ICO**) is responsible for enforcing data protection law, will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

2. Definitions

Key data protection terms used in this data protection policy are:

Personal Information (or 'personal' data)	Any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the school's, or any person's, intentions towards that individual.
Special categories of personal data	Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to

	identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Processing	Virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
Data Processor	An organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
Data Controller	A person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its directors and governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

3. Application of this policy

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

4. Roles and Responsibilities

4.1 Data Protection Lead

The School has appointed Amanda Douglas as the Data Protection Lead who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Lead.

5. The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.

The GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments – where deemed necessary); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

6. Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in our Staff Privacy Notice and Privacy Notice for Parents and Pupils, as GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

7. Headline responsibilities of all staff

7.1 Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that *any* personal data is inaccurate or untrue or if they are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to **record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it**.

7.2 Data handling

7.2.1 Digital Data

Digital information is held securely in the school's management information system (MIS) to enable the school fulfil its statutory and daily tasks quickly and efficiently. This requires the highest level of protection as it contains personal sensitive data under the terms of the Data Protection Act 2018. Accordingly it is only accessible to individuals or groups internal to the school.

- A *Parental Consent Form* must accompany the information provided by a parent
- School staff only may access the MIS, granted on a "need-to-know" basis, with the highest level (administrator) granted to the Headteacher and PA to the Headteacher.
- Personal information is not shared with others without prior consent
- Access is by passwords that change regularly

7.2.2 Hard Copy Data

Personal information held in hard copy format are held in various locations around the school.

The Headteacher and the PA to the Headteacher are the nominated Information Asset Owner(s) (IAO) responsible for the information held in the system and its amendments from time-to-time.

The Headteacher only may issue instructions how and when this data may be shared with others; for example, in the form of reports to secondary schools, or statutory statistical returns to Government departments.

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the Staff Code of Conduct and all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Safeguarding Policy
- Remote Working – Mobile Device Policy
- ICT Acceptable Use Policy
- Data Asset Management and Retention Policy

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

7.3 Sharing Data

From time to time we are legally required to pass on some of this data to others. This includes the Local Authority (LA), another school to which the pupil is transferring, the Department for Education (DfE), the Office for standards in Education (OfSTED), the Independent Schools Inspectorate (ISI) and to the Qualifications and Curriculum Authority (QCA), which is responsible for the National Curriculum and its associated assessment arrangements. Although we are not legally required to, we also pass anonymised information to the independent Schools Council (ISC) and the Independent Schools Association (ISA) in the form of census data.

The Local Authority**,** Oxfordshire County Council, uses information about pupils to carry out specific functions for which it is responsible. For example, participating in the assessing of any special educational needs a pupil may have and any subsequent services it determines to provide. It also uses the information to gather statistics to make essential decisions on, for example, funding pupils in EYFS. For most of the time it uses the data in such a way that individual pupils cannot be identified.

OfSTED and ISI use information about the progress and performance of pupils to help inspectors evaluate the work of schools. To assist schools in their self-evaluation and as part of their assessment of the effectiveness of education initiatives and policy. Inspection reports do not identify individual pupils.

The DfE uses information about pupils for research and statistical purposes; to inform, influence and improve education policy and to monitor the performance of the education service as a whole. The DfE will feed back to LAs and schools information about their pupils for a variety of purposes that will include data checking exercises, use in self-evaluation analyses and where information is missing because it was not passed on by a former school. The DfE will also provide OfSTED and ISI with pupil

level data for use in school inspection. Where relevant, pupil information may also be shared with further education institutions to minimise the administrative burden on application for a course and to aid the preparation of learning plans.

Pupil information may be matched with other data sources that DfE holds in order to model and monitor pupils' educational progression and to provide detailed information back to LAs and learning institutions to support their day to day business. DfE may also use contact details from these sources to obtain samples for statistical surveys - these surveys may be carried out by research agencies working under contract to DfE and participation in such surveys is usually voluntary. The DfE may also match data from these sources to data obtained from statistical surveys.

Pupil data may also be shared with other Government Departments and Agencies including the Office for National Statistics, for statistical or research purposes only. In all these cases the matching will require that individualised data is used in the processing operation in anonymised form. This data sharing will be approved and controlled by the Department's Chief Statistician.

The DFE may also disclose individual pupil information to independent researchers into the educational achievements of pupils who have a legitimate need for it for their research, but each case will be determined on its merits and subject to the approval of the Department's Chief Statistician.

7.4 Avoiding, mitigating and reporting data breaches

One of the key new obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach they must notify Amanda Douglas, Headteacher. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

7.5 Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 5 above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to Amanda Douglas, Headteacher and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

8. Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell Amanda Douglas, Headteacher as soon as possible.

Children, as soon as they are old enough to understand, also have rights under the Act. As a broad guide, it is assumed that most children will have a sufficient understanding by the age of 12. We do not therefore anticipate any such requests from children in Windrush Valley School but where they do occur they will be dealt with promptly and sensitively. Parents have the right to request sight of this information on behalf of their child if he/she is too young to do so themselves.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell Amanda Douglas as soon as possible.

9. Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

- No member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Headteacher.
- No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- No member of staff is permitted to use personal devices for work purposes without prior approval from the Headteacher.

Amanda Douglas
Headteacher
July 2020