Wakefield Grammar School Foundation

Document Reference	**WGSF Data Protection Policy**
Version Number	V1.02
Author/Lead **Job Title**	Vicky Weeks Compliance Manager
Consultation	Jenny Cocker, Director of Finance and Operations
Checker Person Name / Title **Quality Assurance**	Jenny Cocker, Director of Finance and Operations
Name of Approver / Committee **Date Approved**	Risk, Compliance and Governance Committee 14.05.2024
Date of Next Review (annually)	**May 2025**

VALIDITY – Policies should be accessed via FireFly to ensure the current version is used.

CHANGE RECORD - REVIEW PERIOD 1 YEAR

Version	Date	Change details
V1.00	Sept 2018	Policy Written, SWM
V1.01	June 2023	Reviewed and updated in line with ISBA policy Vicky Weeks
V1.02	April 2024	Reviewed against ISBA policy, Vicky Weeks

To be published on the following:

Staff shared	**X**	**School website**	**X**

WGSF Data Protection Policy

1. Background

Wakefield Grammar School Foundation (WGSF), referred to as 'the Foundation', is a family of single-sex independent day schools incorporating Queen Elizabeth Grammar School (QEGS), Wakefield Girls' High School (WGHS) and Wakefield Grammar Pre-Prep, delivering education to children aged 3 - 18.

Data protection is an important legal compliance issue for the Foundation. During the course of the Foundation'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 Foundation's Privacy Notices). The Foundation, as "data controller", is liable for the actions of its staff 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.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (DPA 2018). The DPA 2018 includes 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.

Data protection law has in recent years 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, and 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:

- **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 Foundation (including by its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
- **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.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **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.
- **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.

- **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.

3. Application of this policy

This policy sets out the Foundation'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 Foundation 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 Foundation's personal data as contractors, whether they are acting as "data processors" on the Foundation'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 Foundation 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.

If you are a contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

4. Person responsible for Data Protection at the School

The Foundation has appointed Vicky Weeks, Compliance Manager 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 applicable data protection legislation. 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 (dataprotectionofficer@wgsf.net).

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 Foundation 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); and
- generally having an 'audit trail' of 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, given the relatively high bar of what constitutes consent under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the Foundation 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 Foundation. It can be challenged by data subjects and also means the Foundation is taking on extra responsibility for considering and protecting people's rights and interests. The Foundation's legitimate interests are set out in its Privacy Notice, 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.

6.1 Special Category Data

Article 9 of the UK GDPR gives special protection for certain types of personal data which are considered to be particularly sensitive. These are known as ‘special category data’. These include:

- political opinions
- race
- ethnic origin
- religious or philosophical beliefs
- trade union membership
- genetics
- biometrics (when used for ID purposes)
- health
- sex life or sexual orientation

Foundation staff are required to comply with Article 9 if they intend to process special category data. Article 9 lists the conditions for processing special category data:

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

6.2 Information sharing in an urgent or emergency situation

ICO guidance confirms that 'Data protection law allows organisations to share personal information in an urgent or emergency situation, including to help them prevent loss of life or serious physical, emotional or mental health'. Further information can be found at ICO Information sharing in mental health emergencies at work.

7. Headline responsibilities of all staff

7.1 Record-keeping

It is important that personal data held by the Foundation is accurate, fair and adequate. Staff are required to inform the Foundation if they believe that *any* personal data is inaccurate or untrue or if you 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

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 all relevant Foundation policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the Foundation's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Bring Your Own Device Policy
- CCTV Policy
- Data Retention, Storage and Disposal Policy
- Educational Visits Policy

- ICT Acceptable Use Policy
- Privacy Notices
- Safeguarding and Child Protection Policy
- Social Media Policy
- Use of Images of Pupils 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.

Avoiding, mitigating and reporting data breaches

One of the key 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 Foundation 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 Vicky Weeks, Compliance Manager (and data protection lead).** 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 Foundation always needs to know about them to make a decision.

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

7.3 Care and data security

More generally, we require all Foundation staff (and expect all our contractors) to remain mindful of the data protection principles (see section 3 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 affects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what their 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 Foundation and to identify the need for (and implement) regular staff training. Staff must attend any training we require them to.

7.4 Use of third party platforms / suppliers

As noted above, where a third party is processing personal data on the Foundation's behalf it is likely to be a data 'processor' and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a Data Protection Impact Assessment (DPIA) before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology).

Any request to engage a third party supplier for a platform or software should be referred to IT in the first instance and a software / online services request form submitted. For any request submitted, a due diligence check is carried out by IT and the Compliance Manager to identify any potential issues and the need for a DPIA to be completed.

8. Rights of Individuals

In addition to the Foundation'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 Foundation). 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 Vicky Weeks, Compliance Manager as soon as possible.**

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; and
- 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.

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 Vicky Weeks, Compliance Manager as soon as possible.

9. Data Security: online and digital

The Foundation 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. Please refer to the ICT Acceptable Use Policy.

10. Processing of Financial / Credit Card Data

The Foundation complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Director of Finance and Operations. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such

as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

11. Summary

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?

- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?

- What would be the consequences of me losing or misdirecting this personal data?

- Why am I keeping this personal data? Consider the purpose, is the data still relevant and accurate? Is it stored elsewhere, if so do I really need a copy too? Am I complying with the Data retention and storage policy? Have I considered any safeguarding aspects, Keeping Children Safe in Education will always be the main priority.

- Is the data accessible to unauthorised personnel. E.g. clear desk; kept away from prying eyes; locked away or password protected. If it were my data or that of my children would I be happy with it being stored in this way? How secure is it really? What could I do to make it more secure?

- Can I anonymise the data to reduce the risk of a breach?

Data protection law is best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an important part of the Foundation's culture and all its staff and representatives need to be mindful of it.

If you require further support or information, please contact Vicky Weeks, Compliance Manager (and data protection lead).

Linked Policies

The following privacy notices and policies are all available on FireFly.

- Privacy notice for junior section pupils
- Privacy notice for parent and senior section pupils
- Privacy notice for hirers for facilities
- Privacy notice for staff
- Privacy notice for development, alumni, archives and events
- Data retention and storage policy

APPENDIX 1

GDPR quick guidance document for staff

It is impossible to provide staff with explicit instructions for dealing with every procedure and scenario they encounter in their roles but all staff should be aware of the six key principles for processing data and be mindful of them in their day to day routines.

The dos and don'ts in this document are intended to guide staff and reduce the risk of a data breach but do not form an exhaustive list and staff should speak to Vicky Weeks, Compliance Manager (and data protection lead) if they have any specific queries or concerns.

The GDPR sets out six principles relating to the processing of personal data which must be adhered to. 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.

DO:

- Think how you would expect your or your children's data to be looked after / kept secure;
- Lock computer screens if you leave your desk;
- Regularly change passwords;
- Use secure passwords (e.g. three random words or mixture of upper/lower case/numbers/characters);
- Have a clear desk policy whenever you leave your desk;
- Keep data to what is absolutely necessary to perform the task in hand;
- Keep data secure by locking away in a locked cabinet or office or stored electronically;
- Keep pupil data in staff workrooms rather than classrooms;
- Think about the data – if sensitive be more vigilant;
- Remove identifiers to individuals wherever possible;
- Mark books – electronic is safer (Firefly / Excel), or replace names with initials and reduce information contained;
- Be careful with UCAS forms, due to the amount of personal info entered by students – do not print and do not leave on your screen when dealing with other students. Never share with a third party, e.g. for mock interviews;
- If looking to introduce a new process contact the Data Protection Officer regarding a Data Protection Impact Assessment (DPIA);
- Make data protection a regular agenda item at meetings;
- Be mindful of what data you take home, what you do with it and where you leave it;
- Consider if consent is required, e.g. hoodies student with their names on leavers' hoodies;
- Check students have photography consent (shown on SIMS, see below) before using images. Remember to check on each occasion of use as consent can be withdrawn at any stage.
- Shred all paper waste which contains pupil / staff info – confidential waste can also be added to the security sacks in the Schools' / Foundation offices for safe disposal;
- Regularly go through your emails and delete old ones – save and store as a pdf if you need to retain a record;
- Report to the data protection lead if you think there has been a breach or if you directly receive a subject access request;
- Delete data / images from shared school devices after use, e.g. photos on school cameras, numbers stored in school phones.

DON'T:

- Duplicate records / save copies of data - keep as few copies as possible, as one additional copy doubles the risk of a data breach;
- Print personal data records unless absolutely necessary;
- Print copies of CPOMS entries to store in files;
- Collect data for the sake of it – ensure it has a purpose;
- Give your username or password to anyone;
- Download apps / software without consultation with IT department;
- Sign up to personal accounts using school email addresses;
- Open email attachments from an unknown source (the majority of data breaches do not stem directly from malicious external attackers, they usually originate from an accidental insider);
- Download school data onto personal devices unless first authorised by your employer;
- Work in public spaces where other people could view or overhear personal information – be mindful on trains, etc.;
- Log on to public Wi-Fi whilst working with personal data;
- Enter SEND data in mark books;
- Use email accounts as a storage facility;
- Keep data for longer than necessary or outside the guidelines set out in the data retention, storage and disposal policy;
- Have your emails open when you are projecting to a screen to avoid alerts popping up on the screen;
- Use a pupil name as the subject title for an email;
- Ever allow pupils to work on a computer you are logged onto;
- Email all staff when communicating information about a student that only needs directing towards certain individuals – think before you send.