REDHILL HIGH SCHOOL

- CLYNDERWEN -

Staff Handbook 2023-24

CONTENTS

Schedules:

OUR MISSION STATEMENT

To provide a stimulating and supportive environment for all our students, so that they may be confident, curious and well-rounded young people.

Our Vision

Our vision is simple – to give our students the best possible education.

We will offer a stimulating and purposeful learning experience, so our students become curious, resourceful and confident young people.

We will set high standards of personal conduct and academic rigour, but never at the expense of support and care for each individual, as an individual.

We will expect our teachers to show total commitment to the progress of each learner by understanding their strengths and weaknesses, and encouraging aspiration and ambition at every turn.

We will create a beautiful learning environment for our students, to inspire them every day.

We will help our students to become active and engaged citizens, with a clear moral compass and a charitable ethic.

We will never rest in our desire to be the perfect school.

Overview

1. Introduction

1.1 We are an equal opportunities employer and do not discriminate on the grounds of gender, sexual orientation, marital or civil partner status, pregnancy or maternity, gender reassignment, race, colour, nationality, ethnic or national origin, religion or belief, disability or age.

2. Using the Staff Handbook

2.1 This Staff Handbook sets out the main policies and procedures that you will need to be aware of while working for us. You should familiarise yourself with it and comply with it at all times. Any questions you may have with regard to its contents or what you have to do to comply with it should be referred to The Headmaster.

2.2 The policies and procedures set out in this handbook apply to all staff unless otherwise indicated. They therefore apply to managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff (collectively referred to as **staff** in this handbook).] They do **not** form part of the terms of your contract with us, which are provided to you separately. Your contract sets out your job title, hours and place of work, probationary period, salary, holidays and holiday pay, sickness absence reporting procedure and sick pay, your entitlement to and obligation to give notice to terminate your contract and the duties of confidentiality and restrictions that continue to apply after the termination of your contract.

3. Responsibility for the Staff Handbook

3.1 The Headmaster has overall responsibility for this Staff Handbook and for ensuring that its policies and procedures comply with our legal obligations.

3.2 The Staff Handbook is reviewed regularly to ensure that its provisions continue to meet our legal obligations and reflect best practice.

3.3 Everyone should ensure that they take the time to read and understand the content of this handbook and act in accordance with its aims and objectives. Managers must ensure all staff understand the standards of behaviour expected of them and to take action when behaviour falls below those requirements.

4. Personal details, home address and next of kin

4.1 The Headmaster is responsible for maintaining up-to-date details of the home address, next of kin and emergency contact telephone numbers of each member of our staff.

4.2 We will request this information when you start work and you should advise of any changes straight away. Information is held in confidence and used in accordance with our Data Protection Policy.

Schedule 1 - Dress code

1. About this policy

1.1 We encourage everyone to maintain an appropriate standard of dress and personal appearance at work. The purpose of our dress code is to establish basic guidelines on appropriate clothing and appearance at our workplace, so that we:

(a) promote a positive and professional image;

(b) respect the needs of men and women from all cultures and religions;

(c) make any adjustments that may be needed because of disability;

(d) take account of health and safety requirements; and

(e) help staff decide what clothing it is appropriate to wear to work.

1.2 The Headmaster is responsible for ensuring that this dress code is observed and that a common sense approach is taken to any issues that may arise. Any enquiries regarding the operation of our dress code (including whether an article of clothing is suitable to wear to work) should be made to The Headmaster.

1.3 Failure to comply with the dress code may result in action under our Disciplinary Procedure.

1.4 We will review our dress code periodically to ensure that it reflects appropriate standards and continues to meet our needs.

1.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Appearance

2.1 While working for us you represent us with pupils and parents. Your appearance contributes to our reputation and the development of the school.

2.2 It is important that you appear clean and smart at all times when at work, particularly when you may be in contact with pupils, parents or the general public.

2.3 All employees in public facing roles should wear smart business attire.]

2.4 Employees in public facing roles may be asked to cover up visible tattoos or to remove or cover up visible body piercings.

2.5 You should not wear clothing or jewellery that could present a health and safety risk.

3. Religious and cultural dress

3.1 You may wear appropriate religious and cultural dress (including clerical collars, head scarves, skullcaps and turbans) unless it creates a health and safety risk to you or any other person or otherwise breaches this policy.

3.2 Where necessary Alun Millington can give further information and guidance on cultural and religious dress in the workplace.

3.3 Priority is at all times given to health and safety requirements. Where necessary, advice will be taken from the Headmaster.

Schedule 2 - Equal opportunities policy

1. Equal opportunities statement

1.1 Redhill High School Limited is committed to promoting equal opportunities in employment. You and any job applicants will receive equal treatment regardless of age, disability, gender reassignment, marital or civil partner status, pregnancy or maternity, race, colour, nationality, ethnic or national origin, religion or belief, sex or sexual orientation (**Protected Characteristics**).

2. About this policy

2.1 This policy sets out our approach to equal opportunities and the avoidance of discrimination at work. It applies to all aspects of employment with us, including recruitment, pay and conditions, training, appraisals, promotion, conduct at work, disciplinary and grievance procedures, and termination of employment.

2.2 The Headmaster is responsible for this policy and any necessary training on equal opportunities.

2.3 This policy does not form part of any employee's contract of employment and we may amend it at any time.

3. Discrimination

3.1 You must not unlawfully discriminate against or harass other people including current and former employees, job applicants, clients, customers, suppliers and visitors. This applies in the workplace, outside the workplace (when dealing with customers, suppliers or other work-related contacts or when wearing a work uniform), and on work-related trips or events including social events.

3.2 The following forms of discrimination are prohibited under this policy and are unlawful:

(a) **Direct discrimination:** treating someone less favourably because of a Protected Characteristic. For example, rejecting a job applicant because of their religious views or because they might be gay.

(b) **Indirect discrimination:** a provision, criterion or practice that applies to everyone but adversely affects people with a particular Protected Characteristic more than others, and is not justified. For example, requiring a job to be done full-time rather than part-time would adversely affect women because they generally have greater childcare commitments than men. Such a requirement would be discriminatory unless it can be justified.

(c) **Harassment:** this includes sexual harassment and other unwanted conduct related to a Protected Characteristic, which has the purpose or effect of violating someone's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for them. Harassment is dealt with further in our Anti-harassment and Bullying Policy.

(d) **Victimisation:** retaliation against someone who has complained or has supported someone else's complaint about discrimination or harassment.

(e) **Disability discrimination:** this includes direct and indirect discrimination, any unjustified less favourable treatment because of the effects of a disability, and failure to make reasonable adjustments to alleviate disadvantages caused by a disability.

4. Recruitment and selection

4.1 Recruitment, promotion and other selection exercises such as redundancy selection will be conducted on the basis of merit, against objective criteria that avoid discrimination. Shortlisting should be done by more than one person if possible.

4.2 Vacancies should generally be advertised to a diverse section of the labour market. Advertisements should avoid stereotyping or using wording that may discourage particular groups from applying. They should include a short policy statement on equal opportunities and a copy of this policy will be made available on request.

4.3 Job applicants should not be asked questions which might suggest an intention to discriminate on grounds of a Protected Characteristic. For example, applicants should not be asked whether they are pregnant or planning to have children.

4.4 Job applicants should not be asked about health or disability before a job offer is made, except in the very limited circumstances allowed by law: for example, to check that the applicant could perform an intrinsic part of the job (taking account of any reasonable adjustments), or to see if any adjustments might be needed at interview because of a disability. Where necessary, job offers can be made conditional on a satisfactory medical check. Health or disability questions may be included in equal opportunities monitoring forms, which must not be used for selection or decision-making purposes.

5. Disabilities

5.1 If you are disabled or become disabled, we encourage you to tell us about your condition so that we can consider what reasonable adjustments or support may be appropriate.

6. Part-time and fixed-term work

6.1 Part-time and fixed-term employees should be treated the same as comparable full-time or permanent employees and enjoy no less favourable terms and conditions (on a pro-rata basis where appropriate), unless different treatment is justified.

7. Breaches of this policy

7.1 We take a strict approach to breaches of this policy, which will be dealt with in accordance with our Disciplinary Procedure. Serious cases of deliberate discrimination may amount to gross misconduct resulting in dismissal.

7.2 If you believe that you have suffered discrimination you can raise the matter through our Grievance Procedure or Anti-harassment and Bullying Policy. Complaints will be treated in confidence and investigated as appropriate.

7.3 You must not be victimised or retaliated against for complaining about discrimination. However, making a false allegation deliberately and in bad faith will be treated as misconduct and dealt with under our Disciplinary Procedure.

Schedule 3 - Anti-harassment and bullying policy

8. About this policy

8.1 Redhill High School Limited is committed to providing a working environment free from harassment and bullying and ensuring all staff are treated, and treat others, with dignity and respect.

8.2 This policy covers harassment or bullying which occurs at work and out of the workplace, such as on business trips or at work-related events or social functions. It covers bullying and harassment by staff (which may include consultants, contractors and agency workers) and also by third parties such as customers, suppliers or visitors to our premises.

8.3 This policy does not form part of any employee's contract of employment and we may amend it at any time.

9. What is harassment?

9.1 Harassment is any unwanted physical, verbal or non-verbal conduct that has the purpose or effect of violating a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for them. A single incident can amount to harassment.

9.2 It also includes treating someone less favourably because they have submitted or refused to submit to such behaviour in the past.

9.3 Unlawful harassment may involve conduct of a sexual nature (sexual harassment), or it may be related to age, disability, gender reassignment, marital or civil partner status, pregnancy or maternity, race, colour, nationality, ethnic or national origin, religion or belief, sex or sexual orientation. Harassment is unacceptable even if it does not fall within any of these categories.

9.4 Harassment may include, for example:

(a) unwanted physical conduct or "horseplay", including touching, pinching, pushing and grabbing;

(b) unwelcome sexual advances or suggestive behaviour (which the harasser may perceive as harmless);

(c) offensive e-mails, text messages or social media content;

(d) mocking, mimicking or belittling a person's disability.

9.5 A person may be harassed even if they were not the intended "target". For example, a person may be harassed by racist jokes about a different ethnic group if the jokes create an offensive environment.

10. What is bullying?

10.1 Bullying is offensive, intimidating, malicious or insulting behaviour involving the misuse of power that can make a person feel vulnerable, upset, humiliated, undermined or threatened. Power does not always mean being in a position of authority, but can include both personal strength and the power to coerce through fear or intimidation.

10.2 Bullying can take the form of physical, verbal and non-verbal conduct. Bullying may include, by way of example:

(a) physical or psychological threats;

(b) overbearing and intimidating levels of supervision;

(c) inappropriate derogatory remarks about someone's performance;

10.3 Legitimate, reasonable and constructive criticism of a worker's performance or behaviour, or reasonable instructions given to workers in the course of their employment, will not amount to bullying on their own.

11. If you are being harassed or bullied

11.1 If you are being harassed or bullied, consider whether you feel able to raise the problem informally with the person responsible. You should explain clearly to them that their behaviour is not welcome or makes you uncomfortable. If this is too difficult or embarrassing, you should speak to your line manager, who can provide confidential advice and assistance in resolving the issue formally or informally.

11.2 If informal steps are not appropriate, or have not been successful, you should raise the matter formally under our Grievance Procedure.

11.3 We will investigate complaints in a timely and confidential manner. The investigation will be conducted by someone with appropriate experience and no prior involvement in the complaint, where possible. Details of the investigation and the names of the person making the complaint and the person accused must only be disclosed on a "need to know" basis. We will consider whether any steps are necessary to manage any ongoing relationship between you and the person accused during the investigation.

11.4 Once the investigation is complete, we will inform you of our decision. If we consider you have been harassed or bullied by an employee the matter will be dealt with under the Disciplinary Procedure as a case of possible misconduct or gross misconduct. If the

harasser or bully is a third party such as a customer or other visitor, we will consider what action would be appropriate to deal with the problem. Whether or not your complaint is upheld, we will consider how best to manage any ongoing working relationship between you and the person concerned.

12. Protection and support for those involved

12.1 Staff who make complaints or who participate in good faith in any investigation must not suffer any form of retaliation or victimisation as a result. Anyone found to have retaliated against or victimised someone in this way will be subject to disciplinary action under our Disciplinary Procedure.

13. Record-keeping

13.1 Information about a complaint by or about an employee may be placed on the employee's personnel file, along with a record of the outcome and of any notes or other documents compiled during the process. These will be processed in accordance with our Data Protection Policy.

Schedule 3 Whistleblowing

Please see separate Whistleblowing Policy.

Schedule 4 - Disciplinary and capability procedure

14. About this procedure

14.1 This procedure is intended to help maintain standards of conduct and performance and to ensure fairness and consistency when dealing with allegations of misconduct or poor performance.

14.2 Minor conduct or performance issues can usually be resolved informally with your line manager. This procedure sets out formal steps to be taken if the matter is more serious or cannot be resolved informally.

14.3 This procedure applies to all employees regardless of length of service. It does not apply to agency workers or self-employed contractors.

14.4 This procedure does not form part of any employee's contract of employment and we may amend it at any time.

15. Investigations

15.1 Before any disciplinary hearing is held, the matter will be investigated. Any meetings and discussions as part of an investigation are solely for the purpose of fact-finding and no disciplinary action will be taken without a disciplinary hearing.

15.2 In some cases of alleged misconduct, we may need to suspend you from work while we carry out the investigation or disciplinary procedure (or both). While suspended, you should not visit our premises or contact any of our clients, customers, suppliers, contractors or staff, unless authorised to do so. Suspension is not considered to be disciplinary action.

16. The hearing

16.1 We will give you written notice of the hearing, including sufficient information about the alleged misconduct or poor performance and its possible consequences to enable you to prepare. You will normally be given copies of relevant documents and witness statements.

16.2 You may be accompanied at the hearing by a trade union representative or a colleague, who will be allowed reasonable paid time off to act as your companion.

16.3 You should let us know as early as possible if there are any relevant witnesses you would like to attend the hearing or any documents or other evidence you wish to be considered.

16.4 We will inform you in writing of our decision, usually within 5 working days of the hearing.

17. Disciplinary action and dismissal

17.1 The usual penalties for misconduct or poor performance are:

(a) **Stage 1: First written warning.** Where there are no other active written warnings [or improvement notes] on your disciplinary record, you will usually receive a first written warning. It will usually remain active for six months.

(b) **Stage 2: Final written warning.** In case of further misconduct or failure to improve where there is an active first written warning [or improvement note] on your record, you will usually receive a final written warning. This may also be used without a first written warning [or improvement note] for serious cases of misconduct or poor performance. The warning will usually remain active for 12 months.

(c) **Stage 3: Dismissal or other action.** You may be dismissed for further misconduct or failure to improve where there is an active final written warning on your record, or for any act of gross misconduct. Examples of gross misconduct are given below (paragraph 19). You may also be dismissed without a warning for any act of misconduct or unsatisfactory performance during your probationary period.

We may consider other sanctions short of dismissal, including demotion or redeployment to another role (where permitted by your contract), and/or extension of a final written warning with a further review period.

18. Appeals

18.1 You may appeal in writing within one week of being told of the decision.

18.2 The appeal hearing will, where possible, be held by someone other than the person who held the original hearing. You may bring a colleague or trade union representative with you to the appeal hearing.

18.3 We will inform you in writing of our final decision as soon as possible, usually within one week of the appeal hearing. There is no further right of appeal.

19. Gross misconduct

19.1 Gross misconduct will usually result in dismissal without warning, with no notice or payment in lieu of notice (summary dismissal).

19.2 The following are examples of matters that are normally regarded as gross misconduct:

(a) theft or fraud;

(b) physical violence or bullying;

(c) deliberate and serious damage to property;

(d) serious misuse of the organisation's property or name;

(e) deliberately accessing internet sites containing pornographic, offensive or obscene material;

(f) serious insubordination;

(g) unlawful discrimination or harassment;

(h) bringing the organisation into serious disrepute;

(i) serious incapability at work brought on by alcohol or illegal drugs;

(j) causing loss, damage or injury through serious negligence;

(k) a serious breach of health and safety rules;

(l) a serious breach of confidence.

This list is intended as a guide and is not exhaustive.

Schedule 6 - Grievance procedure

20. About this procedure

20.1 Most grievances can be resolved quickly and informally through discussion with your line manager or The Headmaster. If this does not resolve the problem you should initiate the formal procedure set out below.

20.2 This procedure applies to all employees regardless of length of service. It does not apply to agency workers or self-employed contractors.

20.3 This procedure does not form part of any employee's contract of employment. It may be amended at any time and we may depart from it depending on the circumstances of any case.

21. Step 1: written grievance

21.1 You should put your grievance in writing and submit it to your line manager. If your grievance concerns your line manager you may submit it to The Headmaster.

21.2 The written grievance should set out the nature of the complaint, including any relevant facts, dates, and names of individuals involved so that we can investigate it.

22. Step 2: meeting

22.1 We will arrange a grievance meeting, normally within [one week] of receiving your written grievance. You should make every effort to attend.

22.2 You may bring a companion to the grievance meeting if you make a reasonable request in advance and tell us the name of your chosen companion. The companion may be either a trade union representative or a colleague, who will be allowed reasonable paid time off from duties to act as your companion.

22.3 If you or your companion cannot attend at the time specified you should let us know as soon as possible and we will try, within reason, to agree an alternative time.

22.4 We may adjourn the meeting if we need to carry out further investigations, after which the meeting will usually be reconvened.

22.5 We will write to you, usually within one week of the last grievance meeting, to confirm our decision and notify you of any further action that we intend to take to resolve the grievance. We will also advise you of your right of appeal.

23. Step 3: appeals

23.1 If the grievance has not been resolved to your satisfaction you may appeal in writing to The Headmaster, stating your full grounds of appeal, within one week of the date on which the decision was sent or given to you.

23.2 We will hold an appeal meeting, normally within two weeks of receiving the appeal. This will be dealt with impartially by a [more senior] manager who has not previously been involved in the case. You will have a right to bring a companion (see paragraph 22.2).

23.3 We will confirm our final decision in writing, usually within one week of the appeal hearing. There is no further right of appeal.

Schedule 7 - Sickness absence policy

24. About this policy

24.1 This policy sets out our arrangements for sick pay and for reporting and managing sickness absence.

24.2 Abuse of sickness absence, including failing to report absence or falsely claiming sick pay will be treated as misconduct under our Disciplinary Procedure.

24.3 This policy does not form part of any employee's contract of employment and we may amend it at any time.

25. Reporting when you are sick

25.1 If you cannot attend work because you are sick or injured you should telephone your manager as early as possible and no later than 30 minutes after the time when you are normally expected to start work.

26. Evidence of incapacity

26.1 You must complete a self-certification form for sickness absence of up to seven calendar days.

26.2 For absence of more than a week you must obtain a certificate from your doctor stating that you are not fit for work, giving the reason. You must also complete a self-certification form to cover the first seven days. If absence continues beyond the expiry of a certificate, a further certificate must be provided.

26.3 If your doctor provides a certificate stating that you "may be fit for work" you must inform your manager immediately. We will hold a discussion with you about how to facilitate your return to work, taking account of your doctor's advice. If appropriate measures cannot be taken, you will remain on sick leave and we will set a date for review.

27. Statutory sick pay

27.1 You may be entitled to Statutory Sick Pay (SSP) if you satisfy the relevant statutory requirements. Qualifying days for SSP are Monday to Friday, or as set out in your employment contract. The rate of SSP is set by the government in April each year. No SSP is payable for the first three consecutive days of absence, unless by the Headmaster’s discretion. It starts on the fourth day of absence and may be payable for up to 28 weeks.

28. Return-to-work interviews

28.1 After a period of sickness leave your manager may hold a return-to-work interview with you. The purposes may include:

(a) ensuring you are fit for work and agreeing any actions necessary to facilitate your return;

(b) confirming you have submitted the necessary certificates;

(c) updating you on anything that may have happened during your absence;

(d) raising any other concerns regarding your absence record or your return to work.

29. Managing long-term or persistent absence

29.1 The following paragraphs set out our procedure for dealing with long-term absence or where your level or frequency of short-term absence has given us cause for concern. The purpose of the procedure is to investigate and discuss the reasons for your absence, whether it is likely to continue or recur, and whether there are any measures that could improve your health and/or attendance. We may decide that medical evidence, or further medical evidence, is required before deciding on a course of action.

29.2 We will notify you in writing of the time, date and place of any meeting, and why it is being held. We will usually give you a week's notice of the meeting.

29.3 Meetings will be conducted by your line manager.

29.4 You may bring a companion to any meeting or appeal meeting under this procedure. Your companion may be either a trade union representative or a colleague, who will be allowed reasonable paid time off from duties to act as your companion.

29.5 If you or your companion cannot attend at the time specified you should let us know as soon as possible and we will try, within reason, to agree an alternative time.

29.6 If you have a disability, we will consider whether reasonable adjustments may need to be made to the sickness absence meetings procedure, or to your role or working arrangements.

30. Medical examinations

30.1 We may ask you to consent to a medical examination by a doctor or occupational health professional or other specialist nominated by us (at our expense).

30.2 You will be asked to agree that any medical report produced may be disclosed to us and that we may discuss the contents of the report with the specialist and with our advisers. All medical reports will be kept confidential [and held in accordance with our Data Protection Policy].

31. Initial sickness absence meeting

31.1 The purposes of a sickness absence meeting or meetings will be to discuss the reasons for your absence, how long it is likely to continue, whether it is likely to recur, whether to obtain a medical report, and whether there are any measures that could improve your health and/or attendance.

31.2 In cases of long-term absence, we may seek to agree a return-to-work programme, possibly on a phased basis.

31.3 In cases of short-term, intermittent absence, we may set a target for improved attendance within a certain timescale.

32. If matters do not improve

32.1 If, after a reasonable time, you have not been able to return to work or if your attendance has not improved within the agreed timescale, we will hold a further meeting or meetings. We will seek to establish whether the situation is likely to change, and may consider redeployment opportunities at that stage. If it is considered unlikely that you will return to work or that your attendance will improve within a short time, we may give you a written warning that you are at risk of dismissal. We may also set a further date for review.

33. Final sickness absence meeting

33.1 Where you have been warned that you are at risk of dismissal, and the situation has not changed significantly, we will hold a meeting to consider the possible termination of your employment. Before we make a decision, we will consider any matters you wish to raise and whether there have been any changes since the last meeting.

34. Appeals

34.1 You may appeal against the outcome of any stage of this procedure. If you wish to appeal you should set out your appeal in writing to The Headmaster, stating your grounds of appeal, within one week of the date on which the decision was sent or given to you.

34.2 If you are appealing against a decision to dismiss you, we will hold an appeal meeting, normally within two weeks of receiving the appeal. This will be dealt with impartially and,

where possible, by a more senior manager who has not previously been involved in the case.

34.3 We will confirm our final decision in writing, usually within one week of the appeal hearing. There is no further right of appeal.

34.4 The date that any dismissal takes effect will not be delayed pending the outcome of an appeal. However, if the appeal is successful, the decision to dismiss will be revoked with no loss of continuity or pay.

Schedule 8 - Maternity policy

35. About this policy

35.1 This policy outlines the statutory rights and responsibilities of employees who are pregnant or have recently given birth, and sets out the arrangements for pregnancy-related sickness, health and safety, and maternity leave.

35.2 Arrangements for time off for antenatal care and to accompany a pregnant woman to antenatal appointments are set out in our Time off for Antenatal Appointments Policy.

35.3 In some cases you and your spouse or partner may be eligible to opt into the shared parental leave (**SPL**) scheme which gives you more flexibility to share the leave and pay available in the first year. You will need to give us at least eight weeks' notice to opt into SPL, and you must remain on maternity leave until at least two weeks after birth.

35.4 This policy only applies to employees and does not apply to agency workers or self-employed contractors. This policy does not form part of any employee's contract of employment and we may amend it at any time.

36. Entitlement to maternity leave

36.1 All employees are entitled to up to 52 weeks' maternity leave, consisting of 26 weeks' ordinary maternity leave (**OML**) and 26 weeks' additional maternity leave (**AML**).

37. Notification

37.1 Please inform us as soon as possible that you are pregnant. This is important as there may be health and safety considerations.

37.2 Before the end of the fifteenth week before the week that you expect to give birth (**Qualifying Week**), or as soon as reasonably practical afterwards, you must tell us:

(a) the week in which your doctor or midwife expects you to give birth (**Expected Week of Childbirth**); and

(b) the date on which you would like to start your maternity leave (**Intended Start Date**).

37.3 We will write to you within 28 days to tell you the date we will expect you to return to work if you take your full maternity leave entitlement (**Expected Return Date**).

37.4 Once you receive a certificate from a doctor or midwife confirming your Expected Week of Childbirth (MATB1), you must provide us with a copy.

38. Starting maternity leave

38.1 The earliest you can start maternity leave is 11 weeks before the Expected Week of Childbirth (unless your child is born prematurely before that date).

38.2 If you want to change your Intended Start Date please tell us in writing. You should give us as much notice as you can, but wherever possible you must tell us at least 28 days before the original Intended Start Date (or the new start date if you are bringing the date forward). We will then write to you within 28 days to tell you your new expected return date.

38.3 Your maternity leave should normally start on the Intended Start Date. However, it may start earlier if you give birth before your Intended Start Date, or if you are absent for a pregnancy-related reason in the last four weeks before your Expected Week of Childbirth. In either of those cases, maternity leave will start on the following day.

38.4 Shortly before your maternity leave is due to start we will discuss with you the arrangements for covering your work and the opportunities for you to remain in contact, should you wish to do so, during your leave. Unless you request otherwise, you will remain on circulation lists for internal news, job vacancies, training and work-related social events.

38.5 The law says that we cannot allow you to work during the two weeks following childbirth.

39. Maternity pay

39.1 Statutory maternity pay (**SMP**) is payable for up to 39 weeks provided you have at least 26 weeks' continuous employment with us at the end of the Qualifying Week and your average earnings are not less than the lower earnings limit set by the government each tax year. The first six weeks SMP are paid at 90% of your average earnings and the remaining 33 weeks are at a rate set by the government each year.

39.2 [You will qualify for company maternity pay if you have been continuously employed during the [12] month period ending with the Qualifying Week [and have not received any company maternity pay, adoption pay or shared parental pay from our employment during the [12] month period ending with the Qualifying Week]. This is paid at the rate of your normal basic salary during maternity leave and includes any SMP that may be due for that period.]

39.3 [Payment of company maternity pay is conditional on you confirming in writing, prior to starting maternity leave, that you intend to return to work for at least [six] months. If you later decide not to return to work for this minimum period, you must repay any company maternity pay (but not SMP).]

40. During maternity leave

40.1 With the exception of terms relating to pay, your terms and conditions of employment remain in force during OML and AML.

40.2 Holiday entitlement will continue to accrue during maternity leave. If your maternity leave will continue into the next holiday year, any holiday entitlement that [is not taken **OR** cannot reasonably be taken] before starting your maternity leave can be carried over [and must be taken [immediately before returning to work **OR** within three months of returning to work] unless your manager agrees otherwise]. [You should try to limit carry over to one week's holiday or less. Carry over of more than one week is at your manager's discretion.] Please discuss your holiday plans with your manager in good time before starting your maternity leave. All holiday dates are subject to approval by your manager.

40.3 If you are a member of the pension scheme, we shall make employer pension contributions during OML and any period of paid AML, based on your normal salary, in accordance with the pension scheme rules. Any employee contributions you make will be based on the amount of any maternity pay you are receiving, unless you inform [the Human Resources Department **OR** the Pensions Administrator] that you wish to make up any shortfall.

41. Keeping in touch

41.1 We may make reasonable contact with you from time to time during your maternity leave although we will keep this to a minimum. [This may include contacting you to discuss arrangements for your return to work.]

41.2 You may work (including attending training) on up to ten "keeping-in-touch" days during your maternity leave. This is not compulsory and must be discussed and agreed with your line manager.

41.3 You will be paid at your normal basic rate of pay for time spent working on a keeping-in-touch day and this will be inclusive of any maternity pay entitlement. [Alternatively, you may agree with your line manager to receive the equivalent paid time off in lieu.

42. Returning to work

42.1 You must return to work on the Expected Return Date unless you tell us otherwise. If you wish to return to work earlier than the Expected Return Date, you must give us eight weeks' prior notice of the date. It is helpful if you give this notice in writing. You may be able to return later than the Expected Return Date if you request annual leave or parental leave, which will be at our discretion.

42.2 You are normally entitled to return to work in the position you held before starting maternity leave, and on the same terms of employment. However, if you have taken AML and it is not reasonably practicable for us to allow you to return into the same position, we may give you another suitable and appropriate job on terms and conditions that are not less favourable.

42.3 If you want to change your hours or other working arrangements on return from maternity leave you should make a request under our Flexible Working Policy. It is helpful if such requests are made as early as possible.

42.4 If you decide you do not want to return to work you should give notice of resignation in accordance with your contract.

Schedule 9 – Health and safety policy

43. About this policy

43.1 This policy sets out our arrangements for ensuring we meet our health and safety obligations to staff and anyone visiting our premises or affected by our work.

43.2 The Headmaster has overall responsibility for health and safety and the operation of this policy.

43.3 This policy does not form part of any employee's contract of employment and we may amend it at any time. We will continue to review this policy to ensure it is achieving its aims.

44. Your responsibilities

44.1 All staff share responsibility for achieving safe working conditions. You must take care of your own health and safety and that of others, observe applicable safety rules and follow instructions for the safe use of equipment.

44.2 You should report any health and safety concerns immediately to your line manager or The Headmaster.

44.3 You must co-operate with managers on health and safety matters, including the investigation of any incident.

44.4 Failure to comply with this policy may be treated as misconduct and dealt with under our Disciplinary Procedure.

45. Information and consultation

45.1 We will inform and consult directly with all staff regarding health and safety matters.

46. Training

46.1 We will ensure that you are given adequate training and supervision to perform your work competently and safely.

46.2 Staff will be given a health and safety induction and provided with appropriate safety training, including manual handling, control of substances hazardous to health (COSHH), working at height, asbestos awareness, gas safety, electrical safety and the use of personal protective equipment (PPE)].

47. Equipment

47.1 You must use equipment in accordance with any instructions given to you. Any equipment fault or damage must immediately be reported to your line manager. Do not attempt to repair equipment unless trained to do so.

48. Accidents and first aid

48.1 Details of first aid facilities and the names of trained first aiders are displayed on the notice boards.

48.2 All accidents and injuries at work, however minor, should be reported to The Headmaster and recorded in the Accident Book which is kept in the School Office.

49. Fire safety

49.1 All staff should familiarise themselves with the fire safety instructions, which are displayed on notice boards and near fire exits in the workplace.

49.2 All staff will be trained annually and as required e.g. on induction to follow the Fire Emergency Plan.

49.3 If you hear a fire alarm, leave the building immediately by the nearest fire exit and go to the fire assembly point shown on the fire safety notices.

49.4 Fire drills will be held at least every 12 months and must be taken seriously. We also carry out regular fire risk assessments and regular checks of fire extinguishers, fire alarms, escape routes and emergency lighting.

50. Risk assessments and measures to control risk

50.1 We carry out general workplace risk assessments periodically. The purpose is to assess the risks to health and safety of employees, visitors and other third parties as a result of our activities, and to identify any measures that need to be taken to control those risks.

51. Computers and display screen equipment

51.1 If you use a computer screen or other display screen equipment (DSE) as a significant part of your work, you are entitled to a workstation assessment and regular eyesight tests by an optician at our expense.

51.2 Further information on workstation assessments, eye tests and the use of DSE can be obtained from The Headmaster.

Schedule 10 - Smoking policy

52. About this policy

52.1 We are committed to protecting your health, safety and welfare and that of all those who work for us by providing a safe place of work and protecting all workers, service users, customers and visitors from exposure to smoke.

52.2 All of our workplaces (including our vehicles) are smoke-free in accordance with the Health Act 2006 and associated regulations. All staff and visitors have the right to a smoke-free environment.

52.3 This policy does not form part of any employee's contract of employment and it may be amended at any time.

52.4 If you wish to suggest improvements to the policy or experience particular difficulty complying with it you should discuss the situation with your line manager or The Headmaster.

53. Where is smoking banned?

53.1 Smoking is not permitted anywhere in our workplace. The ban applies to anything that can be smoked and includes, but is not limited to, cigarettes, electronic cigarettes, pipes (including water pipes such as shisha and hookah pipes), cigars and herbal cigarettes.

53.2 No-smoking signs are displayed at the entrances to enclosed or substantially enclosed premises at our workplace.

53.3 Anyone using our vehicles, whether as a driver or passenger, must ensure the vehicles remain smoke-free. Any of our vehicles that are used primarily for private purposes are excluded from the smoking ban.

54. Breaches of the policy

54.1 Breaches of this policy by any employee will be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

54.2 Smoking in smoke-free premises or vehicles is also a criminal offence and may result in a fixed penalty fine and/or prosecution.

Schedule 11 – Privacy policy

Interpretation

Definitions:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

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. Profiling is an example of Automated Processing.

Company name: [LIST TRADING NAME AND INCLUDE GROUP COMPANIES DETAILS IF NECESSARY].

Company Personnel: all employees, workers [contractors, agency workers, consultants,] directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Guidelines: the Company privacy/GDPR related guidelines provided to assist in interpreting and implementing this Privacy Standard and Related Policies, available here: [INSERT LINK TO LIST OF BUSINESS SPECIFIC GUIDELINES OR SET OUT THESE GUIDELINES IN AN APPENDIX].

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing 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.

Related Policies: the Company's policies, operating procedures or processes related to this Privacy Standard and designed to protect Personal Data.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

1. Introduction

This Privacy Standard sets out how Redhill High School ("we", "our", "us", "the Company") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Privacy Standard applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Privacy Standard applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Privacy Standard when Processing Personal Data on our behalf and attend training on its requirements. This Privacy Standard sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Privacy Standard. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Privacy Standard may result in disciplinary action.

This Privacy Standard (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

2. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

Everyone is responsible for ensuring all Company Personnel comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by TBC [NAME], [DEPARTMENT], [TELEPHONE EXTENSION], [EMAIL ADDRESS].]

Please contact the DPO with any questions about the operation of this Privacy Standard or the GDPR or if you have any concerns that this Privacy Standard 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 which you are relying on to process Personal Data (including the legitimate interests used by the Company);

(b) if you need to rely on Consent and/or need to capture Explicit Consent;

(c) if you need to draft Privacy Notices or Fair Processing Notices;

(d) if you are unsure about the retention period for the Personal Data being Processed;

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data;

(f) if there has been a Personal Data Breach;

(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 change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes others than what it was collected for;

(j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;

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

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

5. Personal data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) 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 (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

3. Lawfulness, fairness, transparency

3.1 Lawfulness and fairness

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

the Data Subject has given his or her Consent;

the Processing is necessary for the performance of a contract with the Data Subject;

to meet our legal compliance obligations,

to protect the Data Subject's vital interests;

to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices; or [OTHER GDPR PROCESSING GROUNDS].

You must identify and document the legal ground being relied on for each Processing activity [in accordance with the Company's guidelines on Lawful Basis for Processing Personal Data].

b) Consent

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents 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 are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents so that the Company can demonstrate compliance with Consent requirements.

c) Transparency (notifying data subjects)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Fair Processing Notice which must be presented when the Data Subject first provides the Personal Data..

When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You

must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with the Company's guidelines on Data Retention.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

Security integrity and confidentiality

a) Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data].

b) Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

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.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches - the DPO and follow the Security Incident Response Plan. You should preserve all evidence relating to the potential Personal Data Breach.

Transfer limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

withdraw Consent to Processing at any time;

receive certain information about the Data Controller's Processing activities;

request access to their Personal Data that we hold;

prevent our use of their Personal Data for direct marketing purposes;

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;

restrict Processing in specific circumstances;

challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

request a copy of an agreement under which Personal Data is transferred outside of the EEA;

object to decisions based solely on Automated Processing, including profiling (ADM);

prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

make a complaint to the supervisory authority; and

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.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive the DPO and comply with the company's Data Subject response process.

Accountability

a) The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company must have adequate resources and controls in place to ensure and to document GDPR compliance including:

appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

integrating data protection into internal documents including this Privacy Standard, Related Policies, Privacy Guidelines, Privacy Notices or Fair Processing Notices;

regularly training Company Personnel on the GDPR, this Privacy Standard, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

b) Record keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents [in accordance with the Company's record keeping guidelines.]

These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

c) Training and audit

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training [in accordance with the Company's mandatory training guidelines].

You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

d) Privacy By Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

the state of the art;

the cost of implementation;

the nature, scope, context and purposes of Processing; and

the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data controllers must also conduct DPIAs in respect to high risk Processing.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

Automated Processing including profiling and ADM;

large scale Processing of Sensitive Data; and

large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

an assessment of the necessity and proportionality of the Processing in relation to its purpose;

an assessment of the risk to individuals; and

the risk mitigation measures in place and demonstration of compliance.

[You must comply with the Company's guidelines on DPIA and Privacy by Design.]

e) Automated Processing (including profiling) and Automated Decision-Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

a Data Subject has Explicitly Consented;

the Processing is authorised by law; or

the Processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

[Where you are involved in any data Processing activity that involves profiling or ADM, you must comply with the Company's guidelines on profiling or ADM.]

f) Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

[You must comply with the Company’s guidelines on direct marketing to customers.]

g) Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

they have a need to know the information for the purposes of providing the contracted services;

sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

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

the transfer complies with any applicable cross border transfer restrictions; and

a fully executed written contract that contains GDPR approved third party clauses has been obtained.

[You must comply with the Company's guidelines on sharing data with third parties.]

Changes to this Privacy Standard

We reserve the right to change this Privacy Standard at any time without notice to you so please check back regularly to obtain the latest copy of this Privacy Standard. We last revised this Privacy Standard on [DATE] [and made the following changes: [DETAILS OF CHANGES].

This Privacy Standard does not override any applicable national data privacy laws and regulations in countries where the Company operates. [Certain countries may have localised variances to this Privacy Standard which are available upon request to the DPO.]

Schedule 12 - IT and communications systems policy

55. About this policy

55.1 Our IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards you must observe when using these systems, when we will monitor their use, and the action we will take if you breach these standards.

55.2 The Headmaster has overall responsibility for this policy, including keeping it under review.

55.3 Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

55.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

56. Equipment security and passwords

56.1 You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items that you take out of the office. You should keep your passwords confidential and change them regularly.

56.2 You must only log on to our systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.

56.3 If you are away from your desk you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

57. Systems and data security

57.1 You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

57.2 You must not download or install software from external sources without authorisation from The Headmaster. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

57.3 You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from The Headmaster.

57.4 We monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

57.5 Inform The Headmaster immediately if you suspect your computer may have a virus.

58. E-mail

58.1 Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail. You should also include our standard e-mail signature and disclaimer.

58.2 Remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

58.3 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

58.4 You should not:

(a) send or forward private e-mails at work which you would not want a third party to read;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip;

(c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them; or

(d) send messages from another person's e-mail address (unless authorised) or under an assumed name.

58.5 Do not use your own personal e-mail account to send or receive e-mail for the purposes of our business. Only use the e-mail account we have provided for you.

58.6 [We do not permit access to web-based personal e-mail such as Gmail or Hotmail on our computer systems at any time due to additional security risks.]

59. Using the internet

59.1 Internet access is provided [primarily **OR** solely] for business purposes. [Occasional personal use may be permitted as set out in paragraph 60.]

59.2 You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

59.3 We may block or restrict access to some websites at our discretion.

60. Personal use of our systems

60.1 We permit the incidental use of our systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

60.2 Personal use must meet the following conditions:

(a) it must be minimal and take place [substantially **OR** exclusively] outside of normal working hours (that is, during your lunch break, and before or after work);

(b) personal e-mails should be labelled "personal" in the subject header;

(c) it must not affect your work or interfere with the business;

(d) it must not commit us to any marginal costs; and

(e) it must comply with our policies including the Equal Opportunities Policy, Anti-harassment and Bullying Policy, Data Protection Policy and Disciplinary Procedure.

61. Monitoring

61.1 Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.

61.2 We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

(a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

(b) to find lost messages or to retrieve messages lost due to computer failure;

(c) to assist in the investigation of alleged wrongdoing; or

(d) to comply with any legal obligation.

62. Prohibited use of our systems

62.1 Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

62.2 Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;

(c) a false and defamatory statement about any person or organisation;

(d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

(e) confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);

(f) unauthorised software;

(g) any other statement which is likely to create any criminal or civil liability (for you or us); or

(h) music or video files or other material in breach of copyright.

Schedule 13 Social Media Policy

1. ABOUT THIS POLICY

1.1 This policy is in place to minimise the risks to our business through use of social media.

1.2 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia [, Whisper] [, Instagram] [, Vine] [, Tumblr] and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our business in any way.

1.3 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. PERSONAL USE OF SOCIAL MEDIA

[Personal use of social media is never permitted during working hours or by means of our computers, networks and other IT resources and communications systems.

OR

Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.]

3. PROHIBITED USE

3.1 You must avoid making any social media communications that could damage our business interests or reputation, even indirectly.

3.2 You must not use social media to defame or disparage us, our staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

3.3 You must not express opinions on our behalf via social media, unless expressly authorised to do so by your manager. You may be required to undergo training in order to obtain such authorisation.

3.4 You must not post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

3.5 [You are not permitted to add business contacts made during the course of your employment to personal social networking accounts.

OR

The contact details of business contacts made during the course of your employment are our confidential information. On termination of employment you must provide us with a copy of all such information, delete all such information from your personal social networking accounts and destroy any further copies of such information that you may have.]

3.6 Any misuse of social media should be reported to [POSITION].

4. GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA

4.1 You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address.

4.2 Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

4.3 If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of your employer (unless you are authorised to speak on our behalf as set out in paragraph 3.3). You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

4.4 If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.

4.5 If you see social media content that disparages or reflects poorly on us, you should contact [your manager OR [DEPARTMENT]].

5. BREACH OF THIS POLICY

5.1 Breach of this policy may result in disciplinary action up to and including dismissal. [Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.]

5.2 You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.