Data Protection Policy (incl. Confidentiality, Data Management and CCTV)

Staff, Professionals & Volunteers

Oastlers Policy

Approved by Governing Body On	**February 2019**
To be Reviewed On	**February 2022**
Signed on Behalf of the Governing Body	**Sue Mawson**

Overview

Oastlers School takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship. We intend to comply with our legal obligations under the Data Protection Act 2018 and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to share information contained in this policy.

In the UK, anyone aged 13 and above has the right to:

- Ask to see any data held on them
- Say who else can see data relevant to them

When learners are 16 and above the school cannot share data with parents automatically without the learner's permission.

This policy applies to current and former employees, learners, parent/carers, paid staff, volunteers, apprentices and consultants. If you fall into one of these categories then you are a **'data subject'** for the purposes of this policy. You should read this policy alongside your contract of employment, Service Contract or any one of our Privacy Notices or any other notice we issue to you from time to time in relation to your data.

Aspects of the policy apply specifically to any of the **data subjects** listed above as appropriate. The policy captures the legal framework as it applies to individuals.

Oastlers School has separate policies and privacy notices in respect of job applicants, customers, suppliers and other categories of **data subject**. A copy of these policies and our privacy notices (Appendix 1) can be obtained from the Data Protection Manager, in this case the schools Business Manager, Jeanine Fairbairn.

The school has measures in place to protect the security of your data in accordance with our Data Management Policy which is within this policy. A copy of this can be obtained from Data Protection Manager, Oastlers School. We will only hold data for as long as necessary for the purposes for which we collected it.

Oastlers School is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains how Oastlers School will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of Oastlers School

This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by Oastlers School at any time. It is intended that this policy is fully compliant with the 2018 Data Protection Act and the GDPR and will be reviewed every two years, or sooner where appropriate.

1. Data Protection Principles

Personal data must be processed in accordance with six '**Data Protection Principles**.' What this means is that data must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;

- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

2. How we define personal data

'**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. In this instance **'data subjects'** at Oastlers School include:

- Learners
- Parent/carers
- Staff
- Visitors
- Volunteers
- Visiting professionals
- Suppliers

It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your line manager or other colleagues.

The school, in the course of its duty as your employer will collect and use the following types of personal data about you:

a. recruitment information such as your application form, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
b. your contact details and date of birth;
c. the contact details for your emergency contacts;
d. your gender;
e. your marital status and family details;
f. information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
g. your bank details and information in relation to your tax status including your national insurance number;

h. your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
i. information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
j. information relating to your performance and behaviour at work;
k. training records;
l. electronic information in relation to your use of IT systems/swipe cards/telephone systems;
m. your images (whether captured on CCTV, by photograph or video);
n. any other category of personal data which we may notify you of from time to time.

Personal data for other linked persons may be less detailed according to the nature of the business commissioned by the school

4 Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited1 unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified in section 2.
- One of the special conditions for processing sensitive personal information applies:
  (a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
  (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
  (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
  (d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
  (e) the processing relates to personal data which are manifestly made public by the data subject
  (f) the processing is necessary for the establishment, exercise or defence of legal claims
  (g) the processing is necessary for reasons of substantial public interest
  (h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
  (i) the processing is necessary for reasons of public interest in the area of public health.

The school's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

[1] GDPR, Article 9

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the School can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the GDPR

5 How we define processing

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6 How will we process your personal data?

Oastlers School will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Data Protection Act.

We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 12 below.

We can process your personal data for the purposes above without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of our contract of employment. For example, if you do not provide us with your bank account details we may not be able to pay you. Additionally, an absence of the specific data may prevent us from complying with certain legal obligations and duties which we have with HMRC for example.

7. Examples of when we might process your personal data

It is necessary to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example:

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability;
- to monitor diversity and equal opportunities;
- to monitor and protect the security (including network security) of the school, of you, our other staff and all users of the Oastlers community;
- to monitor and protect the health and safety of you, our other staff, customers and third parties;
- to pay you and provide pension and other benefits in accordance with the contract between us;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions;
- monitoring compliance by you, us and others with our policies and our contractual obligations;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us;
- to answer questions from insurers in respect of any insurance policies which relate to you;
- running Oastlers School and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend Oastlers School in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure;
- for any other reason which we may notify you of from time to time.

We will only process special categories of your personal data in certain situations in accordance with the law. If we seek for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the Data Protection Manager, Oastlers School.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;

- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defense of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

We may process special categories of your personal data as outlined above, where it is necessary to do so. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

We do not take automated decisions about you using your personal data or use profiling in relation to you.

8 Sharing your personal data

Sometimes we may share your personal data with other agencies, such as the Local Authority, DfE or for Safeguarding reasons to carry out our obligations under our contract with you or for our legitimate interests.

We require those agencies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

Legitimate activities which third parties carry out on behalf of Oastlers School are; Payroll with Bradford Metropolitan District Council; Human Resources Support with PACT HR; ICT with Primary Technology.

We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

9. Privacy Notice

The school will issue privacy notices as required, informing data subjects (or their parents/carers, depending on age of the learner, if about learner information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the Data Protection Manager, how and why the school will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. The school must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

The school will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The School will issue a minimum of two privacy notices, one for leaner information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes. (appendix 4 & 5)

10 How should you process personal data for Oastlers School?

Everyone who works for, or on behalf of, Oastlers School has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and Oastlers School Data Security and Data Retention policies.

Oastlers School Data Protection Manager/Data Protection Manager is Jeanine Fairbairn who is responsible for reviewing this policy and updating the Governing Body about data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to Jeanine Fairbairn.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of Oastlers School and only if you are authorised to do so. You should only use data for the specified lawful purpose for which it was obtained and ensure:

- You do not share personal data informally.
- You keep personal data secure and not share it with unauthorised people.
- You regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
- You must not make unnecessary copies of personal data and must keep and dispose of any copies securely.
- You must use strong passwords.
- You lock your computer screens when not at your desk.
- Personal data must be encrypted before being transferred electronically to authorised external contacts. (Speak to IT for more information on how to do this).
- Anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Personal data to your own personal computers or other devices is not stored/saved.
- Personal data is never transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Manager, Jeanine Fairbairn.
- You lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- You do not take personal data away from Oastlers School premises without authorisation from your line manager or Data Protection Manager.
- Personal data is shredded and disposed of securely when you have finished with it.

- You seek help from our Data Protection Manager/Data Protection Manager if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a Subject Access Request (SAR). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

11 How to deal with data breaches

The school has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) the Data Protection Manager will take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

If you become aware of a data breach, you must contact the Data Protection Manager immediately and secure any evidence you have in relation to the breach so the Data Manager can handle the breach as per outlined above.

12 Subject Access Requests

Data subjects can make a '**Subject Access Request**' ('SAR') if you wish to be informed about information we hold about them. This request must be made in writing to the Headteacher (appendix 2).

If you would like to make a SAR in relation to your own personal data you should make this in writing to The Headteacher. The Headteacher will respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for requesting a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request. For more information about SAR's please visit www.ico.org.uk.

14 Your data subject rights

You have the right to information about what personal data we process, how and on what basis as set out in this policy.

You have the right to access your own personal data by way of a SAR.

You can correct any inaccuracies in your personal data. To do so you should contact the Data Protection Manager.

You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the Data Protection Manager.

While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. For this please contact the Data Protection Manager.

You have the right to object to data processing where we are relying on a legitimate interest to do so and you believe that your rights and interests outweigh our own and you wish us to stop.

You have the right to object if we process your personal data for the purposes of direct marketing. Oastlers does not process your data in this way but for further clarification please speak with the Data Protection Manager.

You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

You have the right to be notified of a data security breach concerning your personal data.

In most situations we will not rely on your consent as a lawful ground to process your data. If we do, however, request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Data Protection Manager.

You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

DATA MANAGEMENT POLICY

1. General Principles

1.1 In order to remain compliant with the General Data Protection Regulation (GDPR) 2018 (the Legislation) those handling data on behalf of Oastlers School are expected to:

- Stop and consider whether they should be accessing or disclosing personal data before they do so.
- Individuals handling Oastlers School data must make sure that they have appropriately verified that the person they are passing data on to, is who they say they are and are authorised to receive it. To do this, the identity verification processes should be used
- Not discuss information about colleagues and other stakeholders with unauthorised colleagues, family or friends, or other Oastlers School staff or associates.
- Not access Oastlers Schools records containing personal data other than for a specific business purpose. This may also result in disciplinary action.
- Avoid providing any specific detail about individuals that might lead to their identification when using information for reports or monitoring purposes, unless they have given written permission for it to be used.
- Not express unsubstantiated personal opinions in file notes or e-mails. Individuals may have a right to see the information and may exercise that right.
- Use the blind carbon copy (BCC) option when sending out the same e-mails to others unless recipients have agreed to share their personal email addresses with others on the list.
- Consult the Data Protection Manager before starting any projects involving the processing of personal data.
- Always consider data security and the risks associated with losing personal data, before downloading/printing any personal data.
- Never share a computer password or write it down. Doing so could result in unauthorised access of personal data and, therefore, could constitute a serious security breach.
- Ensure their passwords are created in line with the e-safety and ICT Acceptable Use Policy.
- Always secure devices when leaving unattended – even if it's only for a few minutes. Always remember to log off devices or services at the end of the day or when no longer required.
- Take adequate precautions to protect Oastlers School data in a public place; this includes use of mobile phones, laptops/iPads.
- Be aware that if adequate precautions are not taken by individuals, they are personally accepting the risk of working in this way and the consequences if personal data is left insecure, lost or if there is a complaint.
- Do not to leave documents containing personal data in or on a printer, photocopier or scanner. Fax machines (considered outdated and insecure by the ICO) should not be used to transmit personal data.
- Make sure that personal data cannot be seen or accessed by unauthorised individuals; paper based documents should be stored securely in a lockable cabinet when no longer required.
- If sensitive data is taken out of a building, it needs to be stored in a locked bag or a bag with a padlock.
- When travelling by car, papers must always be transported in a secure part of the car out of sight i.e. in the boot of the car. Papers must not be left in the car overnight; when at home keep them in a locked bag or secured cabinet.

- Dispose of confidential waste and paper copies containing personal data in confidential waste bins or by shredding using a cross cut shredder should be used in all cases). In case of large volumes of confidential waste for homeworkers, contact the Data Protection Manager to ascertain a secure disposal option.
- Encrypt personal data using the Guidance on How to Encrypt a Document.
- Data must only be extracted from the database with prior approval of the line manager and the control of the data whilst extracted is the joint responsibility of the "data extractor" and their manager.
- Those needing to extract more than 1,000 personal data records or 10 sensitive personal data records for Oastlers School processing are to seek the written approval of their manager or Data Protection Manager before proceeding.
- Take **immediate** action in the event of a Data Breach to prevent any further breaches and report any breach to the Data Protection Manager.
- Take responsibility for ensuring your understanding of data protection is current and regularly updated.

2. Transfer of Data to a Third Party Data Processor

2.1 Before personal data is transferred to a third party data processor, a formal written Data Processing Agreement should be in place between Oastlers School and the data processor. This agreement should clearly state the data processors obligation to treat the data in accordance with the provisions of the Legislation, the reasons for the transfer, the time period, what it is required for, how it will be processed and what actions will be taken to delete data when no longer needed.

2.2 Data Processing Agreements are initiated and managed by Oastlers School Data Protection Manager and employees should ensure that they have checked with the Data Protection Manager that a signed Agreement is in place before organising a transfer of personal data to a third party. Note that the Agreement is only valid for the data transfer within the EEA and anything else is not permissible (unless special arrangements are made).

2.3 Once an agreement is in place, data that is to be transferred should be secured. Reasonable precautions should be taken to protect data during the transfer i.e. encryption No electronic or hard copy data files such as case files should be sent through the open post – a secure courier service or special delivery service (includes end to end tracking and signature on delivery) must always be used. The recipient should be clearly stated and the party requesting the information should fund the costs.

2.4 If data is sent via a courier or special delivery, the intended recipient must be advised when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The sender is responsible for ensuring that the confirmation is received, and liaising with the courier service if there is any delay in the receipt of the data.

3. Sending Personal or Sensitive Personal Information Externally

3.1 Through its Customer Relationship Management (CRM) platform (database), Oastlers School processes personal information daily to assist and support its employees. The legislation requires that all departments have appropriate security in place to protect personal information against unlawful or unauthorised use or disclosure, and accidental loss, destruction or damage. The Data Protection Manager is responsible for identifying and adopting appropriate security measures to protect person information stored on the CRM and other data repositories.

3.2 If you have personal information that is currently stored or transferred insecurely, you must secure it immediately.

4. Confidentiality

4.1 The following principles should be followed wherever sensitive personal information is communicated:

- The purpose for sharing the information is justified.
- Information that personally identifies individuals is not used unless necessary.
- Information is only disclosed on a "need to know" basis.
- If unsure then seek guidance on appropriate action from the Data Protection Manager.

4.2 **Face to Face –** Personal information should not be shared in front of others. Employees should ensure that they are not disclosing or requesting the disclosure of sensitive information about themselves or others in front of others, e.g. in reception areas or in a format, that could be viewed by others.

4.3 **Telephone –** Personal information should only be disclosed over the telephone to a third-party where the following procedure has been adhered to:

- The identity of the other party has been confirmed by verification. The type of verification will differ by service and the sensitivity of the information being disclosed.
- The reason for requesting the information has been established and is appropriate.
- Where appropriate, contact details have been requested and their identity checked by calling the person back via the main switchboard of the organisation that they represent and asking for the person by name.
- Provide personal information only to the person who requested it.
- Do not leave any confidential information on voicemail or answering machines as it may be accessible by others. Please remember that by confirming an individual is a member of Oastlers School you may be releasing sensitive personal information as defined by the GDPR.
- When in conversation take precautions to ensure that information is not shared inappropriately with others, e.g. when using mobile phones, travelling on trains, etc.
- Sensitive personal information should not be sent via text messaging as it may be accessible by others.

4.4 Email – Email services should be used as follows:

- Sensitive personal data (or bulk records) must be encrypted if sent via email. There is no need to use encryption when sending an email containing non-sensitive personal data about less than 10 data subjects, unless the data subject themselves insists on all communication being encrypted. Nevertheless, all need to pay attention to detail to ensure that the recipient's email address is spelt correctly to ensure this is delivered to the appropriate person. A test email should always be sent before sending sensitive (or bulk) data for the first time. Bulk data information should not be separated into smaller 'chunks' to avoid the requirement for encryption.
- Care should be taken when addressing email messages to ensure a correct, current address is used and the email is only copied to those with a legitimate interest.
- If information is transmitted and not received by the intended recipient, check that contact details and email address are correct for the receiving party before re-sending.
- Consider the impact on individuals of the data being lost or misdirected. Where information is provided in bulk or where the information is of a sensitive nature make an assessment on the protection to be applied. If in doubt, send information in an encrypted attachment to the email.
- Avoid putting sensitive personal information about more than one person in an email as this will lead to difficulties in maintaining accurate and relevant individual employee's records.
- When transferring data, be aware of who has permission to view your emails or who might be able to view your recipient's inbox.
- When an email does not contain sensitive information relating to a single individual, it does not need to be encrypted.

4.5 Paper – Paper files should be managed as follows:

- A clear desk policy should be observed, wherever possible, at all times. At the end of each day no documents containing personal should be left on a desk.
- All files containing personal data should be held in locked filing cabinets, cupboards or draws. Where the data is sensitive it must be held securely at all times.
- Sensitive documents taken into the public domain must be transported in a locked bag.
- Learners files taken from the secure cupboard must be signed out and returned on the same day.

CONFIDENTIALITY POLICY

At Oastlers School we believe that:

- The safety, well-being and protection of our learners (and their families) are paramount considerations in all decisions staff at this school make about confidentiality. The appropriate sharing of information between school staff is an essential element in ensuring our learners well-being and safety.
- It is an essential part of the ethos of our school that trust is established to enable learners, staff and parents/carers to seek help both within and outside the school.
- Learners, parents/carers, governors and staff need to understand the boundaries of confidentiality in order to feel safe and comfortable discussing personal issues and concerns.
- The school's attitude to confidentiality is easily understood and everyone should be able to trust the boundaries of confidentiality operating within the school.
- Issues concerning personal information and other personal matters can arise at any time.
- Everyone in the school community needs to know that no-one can offer absolute confidentiality.
- Everyone in the school community needs to know the limits of confidentiality that can be offered by individuals within the school community so they can make informed decisions about the most appropriate person to talk to about any health, sex and relationship, safeguarding or other personal issue they want to discuss.
- Matters of Safeguarding and Child Protection override all aspects of confidentiality as per BCSB protocols and procedures.

Definition of Confidentiality

Confidentiality is defined as 'something which is spoken or given in private, entrusted with another's secret affairs'. The confider is asking for the content of the conversation to be kept secret. Anyone offering absolute confidentiality to someone else would be offering to keep the content of his or her conversation completely secret and discuss it with no-one.

In practice there are few circumstances where absolute confidentiality is offered in our school. We strive to strike a balance between ensuring the safety, well-being and protection of our learners and staff, ensuring there is an ethos of trust where learners and staff can ask for help when they need it and ensuring that when it is essential to share personal information, child protection issues and good practice are followed, in accordance with our safeguarding procedures. This means that in most cases what is offered is **limited confidentiality.**

Disclosure of the content of a conversation may be discussed with professional colleagues, but the confider would not be identified except in certain circumstances.

Staff should make it clear that there are limits to confidentiality at the beginning of the conversation. These limits relate to ensuring learner's safety and well-being. The learner will be informed when a confidence has to be broken for this reason and be involved in the information sharing.

Different levels of confidentiality are appropriate for different circumstances:

In the classroom in the course of a lesson given by a member of teaching staff or an outside visitor including health professionals. Careful thought needs to be given to the

content of the lesson setting the climate and establishing ground rules to ensure confidential disclosures are not made. It should be made clear to learners that this is not the time or place to disclose confidential personal information. When a health professional is contributing to a school's health education programme in a classroom setting, they are working with the same boundaries of confidentiality as a teacher.

Disclosures to members of school staff. It is essential all members of staff know the limits of the confidentiality they can offer to both learners and parents and carers and any required actions and sources of further support or help available both for the learner or parent/carer, within the school and from other agencies where appropriate. The needs of the learner are paramount and the school will not automatically share information about the learner with his/her parents/carers unless it is considered to be in the child's best interests.

Disclosures to a counsellor, school nurse or health professional operating a confidential service in the school. Health professionals such as school nurses can give confidential medical advice to learners provided they are competent to do so and follow the Fraser Guidelines (guidelines for doctors and other health professionals on giving medical advice to under 16s). School nurses are skilled in discussing issues and possible actions with young people and always have in mind the need to encourage learners to discuss issues with their parents or carers. However, the needs of the learner are paramount and the school nurse will not insist that a learner's parents or carers are informed about any advice or treatment they give.

Contraceptive advice and pregnancy

The Department of Health has issued guidance (July 2004) which clarifies and confirms that health professionals owe young people under 16 the same duty of care and confidentiality as older patients. It sets out principles of good practice in providing contraception and sexual health to under-16s. The duty of care and confidentiality applies to all under-16s. Whether a young person is competent to consent to treatment or is in serious danger is judged by the health professional on the circumstances of each individual case, not solely on the age of the patient.

However, the younger the patient the greater the concern that they may be being abused or exploited. The Guidance makes it clear that health professionals must make time to explore whether there may be coercion or abuse. Cases of grave concern should be referred through safeguarding procedures.

The Legal Position for School Staff

School staff must not promise confidentiality. Learners do not have the right to expect they will not be reported to their parents or carers and may not, in the absence of an explicit promise, assume that information conveyed outside that context is private. No member of this school's staff can or should give such a promise. The safety, well-being and protection of the child are the paramount consideration in all decisions staff at this school make about confidentiality.

Professional judgement is required by staff, counsellor or health professional in considering whether he/she should indicate to a child that the child could make a disclosure in confidence and whether such a confidence could then be maintained having heard the information. In exercising their professional judgement the teacher, counsellor or health professional must consider the best interests of the child, including the need to both ensure trust to provide safeguards for our children and possible child protection issues.

All Staff at this school receive annual training in safeguarding and are expected to follow the school's safeguarding policies and procedures.

School staff, counsellors and health professionals
At Oastlers School we expect all staff to report any disclosures made by learners or parents/carers of a concerning nature to the designated safeguarding lead as soon as possible after the disclosure and in an appropriate setting, so others cannot over hear. The designated lead for safeguarding will decide what, if any, further action needs to be taken.

Parents/carers
Oastlers School believes that it is essential to work in partnership with parents and carers and we endeavour to keep parents/carers abreast of their child's progress at school, including any concerns about their progress or behaviour. However, we also need to maintain a balance so that our learners can share any concerns and ask for help when they need it. Where a learner does discuss a difficult personal issue with school staff they will be encouraged also (if appropriate in the circumstances) to discuss the matter with their parents or carers and may be supported to do so.

The safety, well-being and protection of our learners are the paramount considerations in all decisions staff at this school make about confidentiality.

Complex Cases
Where there are areas of doubt about the sharing of information, Oastlers School will consult with the Local Authority officers who have specific knowledge of this aspect.

When confidentiality should be broken and the procedures for doing so
See the school's Safeguarding Policy and BCSB website http://bradfordscb.org.uk/

The school Designated Lead for Safeguarding is Lyndsey Brown with Joanne Taylor, Fiona Graham, Ray Sutcliffe and PC Cath Wilkinson as other delegated staff with Safeguarding and Child Protection responsibilities.

Support for Staff
Staff may have support needs themselves in dealing with some of the personal issues of our learners. At Oastlers School we expect staff to ask for help rather than making a poor decision because they lack all the facts or the necessary training, or they risk taking worries about learners home with them.

In all instances, staff are able to seek advice and guidance from any of the schools Safeguarding Leads.

CCTV POLICY

INTRODUCTION

Closed Circuit Television Systems (CCTVS) are installed in Oastlers School.

Any new CCTV systems will be introduced in consultation with staff and governors. Where systems are already in operation, their operation will be reviewed regularly in consultation with senior leaders and governors.

The contact person for anyone wishing to discuss CCTV monitoring is Jeanine Fairbairn on 01274 307456.

1. PURPOSE OF POLICY

"The purpose of this policy is to regulate the use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of Oastlers School.

CCTV systems are installed (both internally and externally) in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day. CCTV surveillance at the school is intended for the purposes of:

- protecting the school buildings and school assets, both during and after school hours;
- promoting the health and safety of staff, learners and visitors;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the school rules are respected so that the school can be properly managed.

2. SCOPE

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material.

3. GENERAL PRINCIPLES

Oastlers School has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, learners and visitors to its premises. The school owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the school community by integrating the best practices governing the public and private surveillance of its premises.

The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.

Information obtained through the CCTV system may only be released when authorised by the Headteacher. Any requests for CCTV recordings/images from the police will be fully recorded and legal advice will be sought if any such request is made If a law enforcement authority, such as the police, is seeking a recording for a specific investigation, the police may require a warrant and accordingly any such request made by the police should be requested in writing and the school will immediately seek legal advice.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school, including Equality & Diversity Policy, Safeguarding policy including Code of Conduct, and Behaviour Policy for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, including the provisions set down in equality and other educational and related legislation.

This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

Video monitoring of public areas for security purposes within school premises is limited to uses that do not violate the individual's reasonable expectation to privacy.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the school or a learner attending the school.

All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by Oastlers School. Recognisable images captured by CCTV systems are "personal data." They are therefore subject to the provisions of the Data Protection Acts 1988, 2003 and 2018.

4. JUSTIFICATION FOR USE OF CCTV

Section 2(1)(c)(iii) of the Data Protection Acts requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected consequently, this means that Oastlers School needs to be able to justify the obtaining and use of personal data by means of a CCTV system. **The use of CCTV to control the internal and external spaces of the school buildings for security purposes has been deemed to be justified by the Governors**.

CCTV systems will not be used to monitor normal teacher/learner classroom activity in school.

5. LOCATION OF CAMERAS

Oastlers School has endeavoured to select locations for the installation of CCTCV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV Video Monitoring and Recording of Public Areas in Oastlers School includes the following:

- ***To promote health and safety of all users.*** Cameras are located in all teaching areas, sports halls, communal areas and the schools designated 'safe spaces'.
- ***Protection of school buildings and property:*** The building's perimeter, entrances and exits, stairwells and corridors, receiving areas for goods/services
- ***Monitoring of Access Control Systems:*** Monitor and record restricted access areas at entrances to buildings and other areas
- ***Verification of Security Alarms:*** Intrusion alarms, exit door controls, external alarms
- ***Video Patrol of Public Areas:*** Parking areas, Main entrance/exit gates
- ***Criminal Investigations (carried out by Police):*** Robbery, burglary and theft surveillance

6. COVERT SURVEILLANCE

Oastlers School will not engage in covert surveillance.

Where the police requests to carry out covert surveillance on school premises, such covert surveillance may require the consent of a judge. Accordingly, any such request made by the police will be requested in writing and the school will seek legal advice.

7. NOTIFICATION – SIGNAGE

The Headtecher will provide a copy of this CCTV Policy upon request to staff, learners, parent/carers and visitors to the school. This policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use. The location of CCTV cameras will also be indicated to the Governing Body. Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to the school. Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

Appropriate locations for signage will include:

- at entrances to premises i.e. external doors, school gates
- reception area
- at or close to each internal camera

8. STORAGE & RETENTION

The General Data Protection Regulation states that personal data must be kept "no longer than is necessary for the purposes for which the personal data are processed" [Art.5(1)(e)]. Oastlers School will only retain CCTV images on the server for 7 days, except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue and is required to assist a criminal investigation or other regulatory body.

All images/recordings are stored in a secure environment with a log of access kept. Access is restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. The Headteacher has delegated the administration of the CCTV System to the Data Protection Manager. In certain

circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above (such individuals may include the police, the Deputy Headteacher, other members of the teaching staff, representatives of the Department of Education and Skills, representatives of the Health & Safety Executive where appropriate). When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis. The school does not authorise the viewing of CCTV images to learners, mon delegated staff or parent/carers unless in exceptional circumstances.

Tapes/DVDs will be stored in a secure environment with a log of access to tapes kept. Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

9. ACCESS

Tapes/DVDs storing the recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to tapes/images will be maintained.

Access to the CCTV system and stored images will be restricted to authorised personnel.

In relevant circumstances, CCTV footage may be accessed:

- By the police where Oastlers School are required by law to make a report regarding the commission of a suspected crime; or
- Following a request by the Police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on Oastlers School property, or
- To the HSE and/or any other statutory body charged with child safeguarding; or
- To assist the Headteacher in establishing facts in cases of unacceptable learner behaviour, in which case, the parents/carers will be informed; or
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to Oastlers School, or
- To individuals (or their legal representatives) subject to a court order.
- To the schools insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

Requests by the Police: Information obtained through video monitoring will only be released when authorised by the Headteacher following consultation with the Chair of Governors. If the Police request CCTV images for a specific investigation, the Police may require a warrant and accordingly any such request made by the Police should be made in writing and the school should immediately seek legal advice.

Subject Access Requests (SAR): On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. To exercise their right of access, a data subject must make a Subject Access Request (SAR) to the Headteacher of the school. The school must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative cost.
Subject access requests can be made to the Headteacher, Lyndsey Brown.

The request should provide all the necessary information to assist the school in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the school. Further information about SAR's can be found at www.ico.org.uk.

In providing the applicant a copy of their data, the school may provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

10. RESPONSIBILITIES

The Headteacher will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by the school.
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within school.
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring at the school is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system
- Ensure that monitoring recorded tapes are not duplicated for release
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. *NOTE: [Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by the Police].*

- Give consideration to both learners and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 7 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Chair of Governors.
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas
- Ensure that where the police request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the Chair of Governors.

11. IMPLEMENTATION & REVIEW

The policy will be reviewed and evaluated from time to time. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, the police, Department for Education, legislation and feedback from parents/carers, learners, staff and others.

12. ADDITIONAL AND NEW CAMERA INSTALLATION

Before the school installs any new CCTV equipment, they will carry out a privacy impact assessment (appendix 3)

APPENDIX 1 – DEFINITIONS

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy;

CCTV – Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.

The Data Protection Acts – The Data Protection Acts 1988, 2003 and GDPR 2018 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All school staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Subject Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.

Data Processing - performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data,
- Retrieving, consulting or using the data,
- Disclosing the data by transmitting, disseminating or otherwise making it available,
- Aligning, combining, blocking, erasing or destroying the data.

Data Subject – an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection Acts place responsibilities on such entities in relation to their processing of the data.

APPENDIX 2 - SUBJECT ACCESS REQUEST FORM

Please complete the following form and return to the Data Protection Manager
DATA SUBJECT DETAILS

Title	
Surname	
First Name(s)	
Current Address	
Telephone (Home)	
Telephone (Work)	
Telephone (Mobile)	
Email address	
Date of Birth	
Details of identification provided to confirm name of data subject in question	
Details of data requested	

If the person requesting the information is NOT the data subject, complete the below:

Are you acting on behalf of the data subject with their written consent or in another legal authority?	YES	NO
If YES please state your relationship with the data subject (eg. parent, legal guardian, solicitor)		
Has proof been provided to confirm you are legally authorised to obtain the information? (eg letter of authority)	YES	NO

Title	
Surname	
First Name(s)	
Current Address	
Telephone (Home)	
Telephone (Work)	
Telephone (Mobile)	
Email address	

Declaration

I hereby request that Oastlers School provide me with the information about the data subject above.

NAME _____ Signed _____ Date_____

APPENDIX 3 - PRIVACY IMPACT ASSESSMENT

Before a school installs a new CCTV system, it is recommended that a documented privacy impact assessment is carried out. A school which properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Acts 1988, 2003 and GDPR 2018. This is an important procedure to adopt as a contravention may result in action being taking against a school by the Office of the Data Protection Commissioner, or may expose a school to a claim for damages from a learner.

Some of the points that might be included in a Privacy Impact Assessment are:

- What is the schools purpose for using CCTV images? What are the issues/problems it is meant to address?
- Is the system necessary to address a pressing need, such as staff and learners safety or crime prevention?
- Are the CCTV cameras intended to operate on the outside of the premises only?
- Is it justified under the circumstances?
- Is it proportionate to the problem it is designed to deal with?
- Is it intended that CCTV cameras will operate inside of the building?
- Are internal CCTV cameras justified under the circumstances?
- Are internal CCTV cameras proportionate to the problem they are designed to deal with?
- What are the benefits to be gained from its use?
- Can CCTV systems realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Does the school need images of identifiable individuals, or could the system use other images which are not capable of identifying the individual?
- Will the system being considered deliver the desired benefits now and remain suitable in the future?
- What future demands may arise for wider use of images and how will they be addressed?
- Is the school, the data controller for the entire CCTV system (bearing in mind that some schools under the PPP are managed for operational purposes by management companies, in which case specific legal advice may need to be sought)?.
- Where a management company is in place, is the school satisfied that it complies with the Data Protection Acts with regard to the processing of images of staff, students and visitors to your school captured on any CCTV systems under its management?
- What are the views of those who will be under CCTV surveillance?
- What could be done to minimise intrusion for those whose images may be captured, particularly if specific concerns have been expressed?
- How have staff, students and visitors been assured by the School that they will not be monitored and that the CCTV system will be used only for the stated purposes?
- Does the school's policy on the use of CCTV make it clear that staff (teaching and non-teaching) will not be monitored for performance or conduct purposes?
- Have the views of staff & learners regarding the location of cameras been taken into account?
- Can the location of each internal camera be justified in accordance with the overall purpose for the use of the CCTV system?

- Has appropriate signage been erected at the location of each internal camera indicating that recording is taking place and outlining the purpose of such recording?
- Who will have access to the system and recordings/images?
- What security measures are in place to protect the CCTV system and recordings/images?
- Are those who will have authorised access to the system and recordings/images clear about their responsibilities?
- Are the camera monitors kept out of view of staff, learners and visitors and is access to the camera monitors restricted to a limited number of staff on a 'need to know' basis?
- Is the room(s) which houses the camera monitors and the CCTV system securely locked when unattended?
- Does the school have a procedure in place to ensure that recordings/images are erased or deleted as soon as the retention period (7 days) has expired?
- Does the school have a procedure in place for handling requests for access to recordings/images from the police?
- Will appropriate notices be in place to ensure that individuals know that they are being monitored?
- Does the school have a data protection policy? Has is been updated to take account of the introduction of a CCTV system?
- Does the school have a procedure in place to handle access requests seeking a copy of images recorded by the CCTV system (within the statutory timeframe of forty days)?
- Has the right of access been communicated to staff, students and visitors?
- Has the school communicated its policy on the use of CCTV to staff, learners and visitors and how has this been done?
- How are new learners and new staff informed of the school's policy on the use of CCTV?

APPENDIX 4

PRIVACY NOTICE FOR SCHOOL WORKFORCE

(THOSE EMPLOYED OR OTHERWISE ENGAGED TO WORK AT THE SCHOOL)

We, Oastlers School, are the Data Controller for the purposes of the General Data Protection Regulations (GDPR).

Personal data is held by the school about those employed or otherwise engaged to work at the school. This is to assist in the smooth running of the school and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector;
- Enabling a comprehensive picture of the workforce and how it is deployed;
- Informing the development of recruitment and retention policies;
- Allowing better financial modelling and planning;
- Enabling ethnicity and disability monitoring; and
- Supporting the network of the School Teacher Review Body and the School Support Staff Negotiating Body.

This personal data includes some or all of the following – identifiers such as name and National Insurance Number and characteristics such as ethnic group, employment contract and remuneration details, qualifications and absence information.

We will not give information about you to anyone outside the school or Local Authority (LA) without your consent unless the law and our rules allow us to.

We are required by law to pass on some of this data to:

- The Local Authority;
- The Department for Education (DfE).

If you require more information about how the Local Authority and/or DfE store and use this data please go to the following website:

- http://www.education.gov.uk/schools/adminandfinance/schooladmin/a0077963/what-the-department-does-with-school-workforce-data
- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you are unable to access these websites, please contact the LA or DfE as follows:

- Information Management Team, City of Bradford MDC
  Margaret McMillan Tower
  Bradford, BD1 1NN
  Email: IMTdatateam@bradford.gov.uk
  Tel: 01274 439652

General enquiries:

- Public Communications Unit, Department for Education
  Sanctuary Buildings, Great Smith Street
  London, SW1P 3BT
  Web: www.education.gov.uk/government/organisations/department-for-education
  Email: http://www.education.gov.uk/help/contactus

  Tel: 0370 000 2288

APPENDIX 5

1. Privacy Notice (How we use learner information)

The categories of learner information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address, parent/guardian)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Medical conditions
- Special Educational Needs and Disability
- Behaviour and exclusions
- Education/school history
- Siblings information

Why we collect and use this information

We use the learner data:

- to support learner learning
- to monitor and report on learner progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to safeguard learners

The lawful basis on which we use this information

On the 25th May 2018 the Data Protection Act 1998 was replaced by the General Data Protection Regulation (GDPR). The condition for processing under the GDPR will be:

Article 6

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(c) Processing is necessary for compliance with a legal obligation to which the controller is subject;

Article 9

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:

(j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The Education (Information about Individual Pupils) (England) Regulations 2013 - Regulation 5 'Provision of information by non-maintained special schools and Academies to the Secretary of State' states 'Within fourteen days of receiving a request from the Secretary of State, the proprietor of a non-maintained special school or an Academy (shall provide to the Secretary of State such of the information referred to in Schedule 1 and (where the request stipulates) in respect of such categories of pupils, or former pupils, as is so requested.'

The Education Act 1996 - Section 537A – states that we provide individual pupil information as the relevant body such as the Department for Education.

Children's Act 1989 – Section 83 – places a duty on the Secretary of State or others to conduct research.

Collecting learner information

Whilst the majority of learner information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing learner data

We hold learner data for the duration of time each the child remains at Oastlers School.

Who we share learner information with

We routinely share learner information with:

- schools that the learner's attend after leaving us
- our local authority
- the Department for Education (DfE)
- NHS/school nurse
- Third party professional services i.e. West Yorkshire Police, Children's Social Care, Youth Offending Team, School Nursing Service, CAMHS, Connexions, Alternative Providers/College.

Why we share learner information

We do not share information about our learners with anyone without consent unless the law and our policies allow us to do so.

We share learners' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our learners with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

Learners aged 13+

Once our learners reach the age of 13, we also pass learner information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by

informing us. This right is transferred to the child / learner once he/she reaches the age 16.

Learners aged 16+

We will also share certain information about learners aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers
- For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our learners from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to learner information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and learners have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact The Business Manager.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

2. Contact

If you would like to discuss anything in this privacy notice, please contact:

Mrs Jeanine Fairbairn
Business Manager
Oastlers School
Flockton Road
Bradford
BD4 7RH

3. Privacy Notice (How we use learner information)

Declaration

I, _____, parent /carer of _____
declare that I understand:

- Oastlers School has a legal and legitimate interest to collect and process my personal data in order to meet statutory requirements.
- How my data is used.
- Oastlers School may share my data with the DfE, and subsequently the LA.
- Oastlers School will not share my data to any other third parties without my consent, unless the law requires the school to do so.
- Oastlers School will always ask for explicit consent where this is required, and I must provide this consent if I agree to the data being processed.
- My data is retained in line with the school's GDPR Data Protection Policy.
- My rights to the processing of my personal data.
- Where I can find out more information about the processing of my personal data.

Consent

At Oastlers School, we store and use personal information to educate and care for learners in school, including those to be placed at the school and those learners who have recently left.

Photographs	The school can take, or arrange to have taken, photographs for use in school to enable staff to identify learners. This is part of our role of educating and caring for learners.	No parental consent required
	The school will take, or arrange to have taken, photographs that will be used for internal and external documents. These include newsletters, pamphlets and photographs of sports and activities. These photographs may be used on the school website and in published documents in relation to school.	As a parent, I consent for photographs to be used of my child as detailed Yes ☐ No ☐

This consent can be withdrawn at any time by contact office@oastlers.co.uk

Signed _____ Date _____

Relationship to Learner _____