



CODE OF CONDUCT FOR WORKING WITH CHILDREN POLICY

VERSION 7.0

Status	Non-statutory
Responsible committee/Individual	Trust Board
Author	CEO
Target Audience	All stakeholders
Date Policy Agreed	February 2020 – Version 1 July 2020 – Version 2 December 2020 – Version 3 May 2021 – Version 4 December 2023 – Version 5 December 2024 – Version 6 December 2025 – Version 7
Review Date	December 2026

CONTENTS

Page Number

Aims, Scope and Principles	2
Legislation and Guidance	2
General Obligations	2
Safeguarding	3
Reporting Incidents	3
Diversity	4
The Trust's Commitment	4
Personal Conduct	4
• Confidentiality	4
• Making a Professional Judgement	4
• Personal/Living Space	5
• Gifts, Rewards and Favouritism	5
• Infatuations	5
• Communication (including the use of Technology)	5
• Social Contact	6
• Sexual Contact	6
• Physical contact	6
• Behaviour Management	7
• Personal/Intimate Care	7
• Staff Dress and Appearance	7
• First Aid and the Administration of Medicine	7
• One to One Situations/Home Visits	8
Transport and Car Usage – Staff Responsibilities	8
Car Usage – Safeguarding	9
Trips and Outings	9
E-Safety, Use of ICT, Photocopying and Videos	10
Extremism, Radicalisation and Political Views	11
Monitoring Arrangements	12
Appendix A – Acceptable Usage Agreement	13

CODE OF CONDUCT FOR WORKING WITH CHILDREN

1. Aims, Scope and Principles

This guidance document describes the standards of conduct and practice that the Brighter Futures Learning Partnership Trust (The Trust) staff and volunteers should follow when working with children. It is designed to complement other advice or codes of conduct produced by employers or national bodies, not to replace or take priority over them.

By creating this policy, we aim to ensure our Trust provides an environment where everyone is safe, happy and treated with respect. Whilst this policy covers a wide range of situations, it is recognised that it cannot cover every eventuality, however the principles contained within it must apply in every circumstance.

Many of the principles in this code of conduct are based on the Teachers' Standards and therefore, this policy should be read in conjunction with these standards.

School staff have an influential position in school and will act as role models for students/pupils by consistently demonstrating high standards of behaviour and dress. We expect that all teachers will act in accordance with the personal and professional behaviours set out in the Teacher Standards. We expect all support staff, governors and volunteers to also act with personal and professional integrity, respecting the safety and well-being of others.

2. Legislation and Guidance

In line with statutory safeguarding guidance 'Keeping Children Safe in Education', we should have a staff code of conduct which covers acceptable use of technologies, staff/student/pupil relationships and communication, including the use of social media. This policy is linked to each school's safeguarding, e-safety, acceptable use of technology policies.

This policy also links to the Trust's Funding Agreement and the Articles of Association.

3. General Obligations

All adults who have contact with children and young people, in their work, have a legal and moral duty to keep them safe, protecting them from sexual, physical and/or emotional harm. The duty that rests on an individual is to ensure that all reasonable steps are taken to ensure the welfare of a child or young person is paramount.

Staff will, therefore:

- Keep children safe by clarifying which behaviours constitute safe practice and which behaviours should be avoided.
- Assist adults working with children to work safely and responsibly and to monitor their own standards and practice.
- Support managers in setting clear expectations of behaviour and/or codes of practice relevant to the services being provided.

- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Support safer recruitment practice.
- Minimise the risk of misplaced or malicious allegations made against adults who work with children.
- Reduce the incidence of positions of trust being abused or misused.

It is important that staff are role models for students/pupils. They will:

- Maintain high standards in their attendance and punctuality.
- Never use inappropriate or offensive language in school.
- Show tolerance and respect for the rights of others.
- Not undermine fundamental British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs.
- Express personal beliefs in a way that will not overly influence students/pupils and will not exploit students'/pupils' vulnerability or might lead them to break the law.
- Understand the statutory frameworks they must act within.

Failure to follow the code of conduct may result in disciplinary action being taken, as set out in the Trust's disciplinary procedures.

Please note that this code of conduct is not exhaustive. If situations arise that are not covered by this code, staff will use their professional judgement and always in the best interest of the Trust and its students/pupils.

4. Safeguarding

Staff have a duty to safeguard students/pupils from harm, and to report any concerns they have. This includes physical, emotional and sexual abuse, or neglect.

Staff will familiarise themselves with their school's safeguarding policy and procedures and the Prevent initiative, ensuring they are aware of the processes to follow if they have concerns about a child.

Safeguarding policies and procedures **are available in each staff room and** from the school admin office. New staff will also be given copies on arrival to the Trust as part of the induction process.

5. Reporting incidents

Staff should report any safeguarding concerns about another colleague's behaviour to their Headteacher. If there are safeguarding concerns about the Headteacher or another member of the Trust, these should be reported to the CEO. If there are safeguarding concerns about the CEO, these should be reported to the Chair of the Trust by emailing Mrs Steel, the Executive Personal Assistant to the CEO (executivepa@brighterfutureslpt.com)

In cases where there is an allegation or risk of harm to a child this must be reported to the Child Protection Officer in school.

6. Diversity

At all times consideration needs to be given to the diverse needs of staff and children. Aspects of gender, culture or religion may be relevant when considering the nature of allegations or appropriateness of communications or physical interventions.

7. The Trust's Commitment

The Trust will ensure:

- Appropriate safeguarding and child protection policies and procedures are in place in all areas that undertake work with children, that they are continually monitored and reviewed and made easily accessible to all staff.
- Staff are treated fairly and reasonably in all circumstances and if subject to an allegation will be supported and the principles of natural justice applied.
- The safe practice of staff is continually promoted through supervision and training.
- Staff have readily available access to senior management or other emergency contacts.
- Guidance is readily available to both adults and children.
- A culture of openness and support is fostered.
- Readily known systems are in place for situations and concerns, from either party, to be raised and recorded and for their outcomes to be analysed in order to review procedures and working practices.
- A clear E-Safety policy is in place.
- A clear and easily accessible Whistle Blowing policy is in place which is available on the Trust website and in each school's office.

8. Personal Conduct

Confidentiality

Staff must:

- Ensure that private and sensitive information should only be shared with appropriate adults.
- Not use information to intimidate, humiliate or embarrass the child.
- Be aware of the need to listen and support children whilst understanding the importance of not promising to keep secrets.
- Never request a child keeps secrets.

Making a Professional Judgement

Staff must:

- Act professionally and always in the best interests of the child.
- Discuss any concerns or threats with a senior manager.
- Be aware of their position of trust and ensure an unequal balance of power is not used for their own or others personal advantage or gratification.
- Not use their position to intimidate, bully, humiliate, threaten, coerce or undermine children.

- Maintain appropriate professional boundaries and avoid behaviour which might be misinterpreted by others.
- Not promote relationships which create a personal friendship or are of a sexual nature, or which may become so.
- Ensure that policies referring to social networking, confidentiality and health and safety are applied.

Personal/Living Space

Staff must:

- Not invite a child into their home or any home or domestic setting frequented by them, unless the reason for this has been firmly established and agreed with parents and senior managers or the home has been designated as a workplace e.g. childminders, foster carers.
- Be vigilant in maintaining their own privacy and mindful of the need to avoid placing themselves in vulnerable situations.
- Not ask children to undertake personal jobs or errands.
- Maintain professional boundaries.

Gifts, Rewards and Favouritism

Staff must:

- Follow the school's policy on the giving and receiving of gifts.
- Only give gifts to an individual child as part of an agreed reward system.
- Ensure that when operating reward systems, methods and criteria for selection of children for awards are fair and transparent.

Infatuations

Staff must:

- Deal with infatuations sensitively and appropriately to maintain the dignity and safety of all concerned and report to their line manager.
- Make sure their own behaviour is beyond reproach.

Communication (including the use of Technology)

Staff must:

- Ensure communication takes place within clear and explicit professional boundaries; this includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, webcams, websites and blogs.
- Not share any personal information with a child including personal contact details.
- Not request, or respond to, any personal information from a child, other than that which may be appropriate as part of their professional role.
- Never share personal information disclosed by a child with their siblings or any other family members, unless deemed appropriate by senior leaders as part of their professional role.
- Not give their personal contact details to children, including their mobile number, home phone or personal e-mail address, unless the need to do so is agreed with senior management and parents.

- Not use personal equipment, e.g. mobile phones even when parents/carers have given permission.
- Only make contact with children for professional reasons and in accordance with school policy.
- Use internal e-mail systems in accordance with each school's policy.

Social Contact

Staff must:

- Not have social contact with children unless the reason for this has been firmly established and agreed with parents.
- Alert senior management of any social contact that has occurred which may raise concern.
- Report and record any situation which may place a child at risk or may compromise the school or their own professional standing.

Sexual Contact

Staff must:

- Not engage in sexual activity with or in the presence of a child, or cause or incite a child to engage in or watch sexual activity, to do so would be considered a criminal offence.
- Not have any form of communication which could be interpreted as sexually suggestive or provocative or make sexual remarks to, or about a child either verbally, written or electronically.
- Not discuss their own sexual relationships with or in the presence of children.
- Ensure relationships take place within boundaries of respect and professionalism.
- Ensure language, attitudes and demeanour do not give rise to comment or speculation.
- Be aware that consistently conferring in appropriate special attention and favour upon a child might be construed as part of a grooming process, and as such will give rise to concerns about behaviour.

Physical Contact

Staff must:

- Be aware that even well-intentioned physical contact may be misconstrued by the child, an observer or by anyone to whom this action is described.
- Only have physical contact with a child when it is necessary and in ways which are appropriate to their professional or agreed role and responsibilities, never touch a child in a way which may be considered indecent.
- Be aware of the child's reactions or feelings and, as far as possible, only use a level of contact which is acceptable to the child and for the minimum time necessary.
- Not assume that when a child is distressed, they seek physical comfort.
- Always encourage children, where possible to undertake self-care tasks independently.
- Be aware of cultural or religious views about touching and sensitive to issues of gender.
- Where there is regular physical contact needed, the nature of this must be agreed with the parent as part of a formally agreed plan.

- Where a child initiates inappropriate physical contact, you must sensitively deter them and help them understand the importance of personal boundaries. This must be reported immediately to the Child Protection Officer.

Behaviour Management

Staff must:

- Not use any form of degrading treatment to punish a child.
- Not use demeaning or insensitive comments.
- Use humour with care.
- Ensure any sanctions and rewards are part of an agreed behaviour management policy.
- Try to defuse situations before they escalate.
- Never use corporal punishment.
- Follow the behaviour policy and only use physical intervention as a last resort, when other behaviour management strategies have failed and where there is a risk of physical injury or serious damage to property.
- When, using physical intervention, use the minimum force necessary and always report and document the incident.
- Be mindful of other factors which may be impacting on a child's behaviour, e.g. bullying, changes in home circumstances.

Note: the use of unwarranted physical force is likely to constitute a criminal offence.

Personal/Intimate Care

Staff must:

- Respect children's privacy at all times.
- Avoid any physical contact when children are in a state of undress, other than as part of an agreed care plan.
- Not change in the same place as children.
- Not shower or bathe with children.
- Not assist with any personal care task which a child can undertake themselves.

Staff Dress and Appearance

Staff must:

- Present a professional image of the school.
- Model appropriate dress as an example to learners and visitors.
- Not wear excessively revealing clothes.
- Not wear anything which is likely to bring the school into disrepute, e.g. potentially offensive badges, logos or motifs, political slogans.

First Aid and the Administration of Medicine

Staff must:

- Be suitably trained and qualified before administering first aid and/or any agreed medication.
- Ensure arrangements are in place to obtain parental consent for the administration of medication.

- Adhere to each school's policy.
- Explain to the child what is happening.
- Ensure parents are kept informed as appropriate.
- Inform the Headteacher/SLT immediately if an ambulance is required.

For more severe accidents/health concerns, notify the Headteacher/SLT immediately if contact cannot be made with the parents/carers.

One to One Situations/Home Visits

Staff must:

- Ensure that, when lone working is an integral part of their role, full and appropriate risk assessments are in place.
- Avoid meetings with a child in secluded areas.
- Always inform colleagues and/or parents about one-to-one contact beforehand, assessing the need to have them present or close by.
- Avoid the use of engaged or equivalent signs, wherever possible, these create an opportunity for secrecy or the interpretation of secrecy.
- Carefully consider the need of the child when in a one-to-one situation and always report any situation where the child becomes distressed or angry towards you.
- Agree the purpose for any home visit with the line manager unless it is an acknowledged and integral part of your role.
- Be alert to the possible consequences of being in a one-to-one situation when little or no information is available about the child.

9. Transport and Car Usage – Staff Responsibilities

If using a vehicle to carry out responsibilities associated with his/her employment a worker must ensure that he/she:

- Adheres to the Highway Code and Health and Safety Legislation.
- Conforms with his/her insurance company that the vehicle is insured for business use (note: vehicles used for business use must be insured for that purpose, not just commuting to and from work).
- The car used has vehicle excise duty paid, is roadworthy and has a current MOT (if more than 3 years old).
- Has a current full driving licence, appropriate to the vehicle being driven.
- Carries out regular basic maintenance checks such as oil, water, washer fluid, wipers, lights.
- Horn, tyre condition and pressures and properly functioning seat belts.
- The vehicle is suitable for its purpose and expected mileage.
- Advises his/her manager if he/she is charged with any motoring offence or he/she incurs any penalty points on his/her driving licence or if he/she becomes disqualified from driving. Failure to do so may result in disciplinary action.
- Reports any accidents arising in the course of employment to his/her line manager and the Health and Safety Manager. Failure to do so may result in disciplinary action.

- Always wears a seat belt.
- All equipment carried should be secured to prevent any movement likely to endanger driver and/or passenger/s.
- Ensure adequate time to make journeys safely with appropriate rest breaks (the Highway Code advises a 15-minute break every 2 hours).
- Advises his/her line manager if he/she has a medical condition that effects his/her ability to drive, or he/she believes he/she is unfit to drive for any reason and seeks appropriate medical advice.
- Never use a mobile phone when driving – hands free devices must not be used.
- Advises their manager/colleagues where they are going and expected return time.

10. Car Usage – Safeguarding

Where a member of staff is transporting a student, the following must also be adhered to:

- Staff using their own vehicle must complete a Trust Voluntary Vehicle Use form.
- Written permission (letter or email) must have been given by the parent.
- Where possible, the child should sit in the back of the vehicle (children who get car sick in the back can be an exception to this).
- There must be a record of the journey route, and the employee's line manager and child's parents must be aware of this.
- Staff transporting children should have a first aid kit, their work ID and a mobile phone in the car at all times.
- Staff must never leave a child unattended in their car.
- Staff must ensure that all children have appropriate restraints for their age.
- Where possible, staff should alternate driving duties, to prevent one person always being alone with the same child or group of children.

11. Trips and Outings

Staff must:

- Recognise that they are in a position of trust and ensure that their behaviour remains professional at all times and stays clearly within defined boundaries.
- Ensure staff/child ratios and gender mix are appropriate.
- Always have another adult present in out of school activities, unless otherwise agreed with a senior manager.
- Ensure risk assessments are undertaken.
- Have parental consent to the activity.
- Not share bedrooms with children unless in exceptional circumstances where parents have given agreement and there are two members of staff present at all times.
- Ensure that the trips/visits' policies are followed.
- Not act in any way that will bring the Trust or the teaching profession into disrepute. This covers relevant criminal offences, such as violence, sexual misconduct, inappropriate use of alcohol as well as any negative comments about any of the schools in the Trust.

12. E-Safety, Use of ICT, Photocopying and Videos

Staff must:

- Be clear about the purpose of any activity involving photography and what will happen to the images when the activity is concluded.
- Be able to justify the reason for having images of children in their possession.
- Avoid making images in one-to-one situations or situations that may be construed as harmful, or which show a single child with no surrounding context.
- Immediately report any concerns if any inappropriate or intrusive images are found.
- Have parental consent to take, display and/or distribute any images of children.
- Not use images that may cause distress or offence.
- Not access, make or store indecent images of children on the internet or other devices including personal equipment, to do so would be illegal and lead to a criminal investigation.
- Ensure that children are not exposed to unsuitable material through ICT.
- Ensure that any materials shown to children are age appropriate.
- Immediately report any concerns, if any inappropriate or intrusive images are found, to the Child Protection Officer and the E-safety co-ordinators.
- Not use personal devices for photography or videos. You will only use approved school devices.
- Have an up-to-date awareness; of e-safety matters and of the school's current e-safety Policy and practices.
- Have read and understood the appropriate ICT agreements.
- Ensure e-safety issues are embedded in all aspects of the curriculum and other school activities.
- Ensure students understand and follow the school's e-safety and Acceptable Use Policy.
- Ensure students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Ensure they monitor ICT activity in lessons, extra-curricular and extended school activities.
- Ensure they are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current best practice regarding these devices.
- Ensure that in lessons where internet use is pre-planned, students should be guided to sites that are checked as suitable for their use and that processes are in place to deal with any unsuitable material that is found in internet searches.
- Report any suspected misuse or problem to a member of SLT and the ICT Support Manager.
- Ensure that digital communications with students are only on a professional level and carried out using official school systems.
- Maintain a formal and courteous and professional tone in communicating with students and ensure that professional boundaries are always maintained.
- Only use official channels of communication e.g. Office 365 and work e-mail addresses and be aware of and comply with the school's policies and guidance.
- Not exchange private text, phone numbers, personal e-mail addresses or photos of a personal nature with students.
- Firmly decline student-initiated 'friend' requests from students and not instigate any. Use discretion when dealing with friend requests from parents. It is acceptable to decline these invitations and remind parents of more formal channels on which they can discuss their child's education.

- Operate online in a way which would not call into question their position as a professional.
- Manage privacy settings and keep them under review. These are particularly important regarding photos and remember that no privacy mechanism is 100% guaranteed.
- Ensure settings prohibit others from tagging them in any photos or updates without explicit permission. Staff must always ask others to remove any undesirable content related to them.
- Be aware that potential employers may try and view your online social media profiles.
- Consider that conversations held online may not be private. Be aware of who may have access to what is posted.
- Assume that information posted can be accessed and altered.
- Not discuss students, colleagues, parents or carers online or criticise your employer or others within the school community.
- Respect student privacy and confidentiality always.
- Use strong passwords and change them regularly. Protect mobile phones, smart phones/tablet computers with a PIN, especially when in school to protect access to its content and potential misuse.
- Bring the matter to the attention of the Headteacher using the proper procedures, if they are the victim of cyber bullying or are uncomfortable with comments, photos or posts made by students in relation to them.
- Audit and re-evaluate the information about them and who has access to it if they are entering a programme of teacher education, or Teacher Induction Period.

It is understood that social media can play an important part in communication between the school and students, parents/carers; however, there is also a need to ensure it is used in an appropriate and safe way. Before any member of staff sets up a resource such as a student blog space or a school Twitter account, they must seek permission from the Headteacher, and they should ensure that appropriate steps are taken to make such social media 'private' so that only people they approve can access it. The member of staff will then be responsible for the posts made on the site and for moderating the content from other users/contributors.

13. Extremism, Radicalisation and Political Views

The Trust values freedom of speech and the expression of beliefs/ideology as a fundamental right underpinning our society's values. Both students and staff have the right to speak freely and voice their opinions. However, freedom comes with responsibility and free speech that is designed to manipulate the vulnerable or that incites or leads to violence or harm to others goes against the moral principles in which freedom of speech is valued. Free speech is not an unqualified privilege; it is subject to laws and policies governing equality, human rights, community safety and community cohesion.

The threat from terrorism in the United Kingdom may include the exploitation of vulnerable people to involve them in terrorism or in activity in support of extremism and terrorism. The normalisation of extreme views may also make children and young people vulnerable to future manipulation and exploitation. The Trust is clear that this exploitation and radicalisation should be viewed as a safeguarding concern.

The Trust recognises that extremism and exposure to extremist materials and influences can lead to poor outcomes for students and so this should be addressed as a safeguarding concern as set out in

this policy. We also recognise that if we fail to challenge extremist views, we are failing to protect our students.

Extremists of all persuasions aim to develop destructive relationships between different communities by promoting division, fear and mistrust of others based on ignorance or prejudice and thereby limiting the life chances of young people. Education is a powerful weapon against this; equipping young people with the knowledge, skills and critical thinking, to challenge and debate in an informed way. Therefore, the Trust will provide a broad and balanced curriculum, delivered by skilled professionals, so that our students are enriched, understand and become tolerant of difference and diversity and also to ensure that they thrive, feel valued and not marginalized.

The Trust will closely follow any locally agreed procedures as set out by Doncaster Metropolitan Borough Council for safeguarding individuals vulnerable to extremism and radicalisation.

The Trust have determined “British Values” to be:

- Democracy
 - The rule of law
 - Individual liberty
 - Mutual respect
 - Tolerance of those with different faiths and beliefs
-
- The Trust aim to develop and nurture these by:
 - Planning assemblies and curriculum programmes where core ethical values and beliefs are considered.
 - Well-structured PSHE curriculum delivered in tutor time across all age ranges throughout the academic year. The PSHE programmes will address fundamental British Values and the Core Values. These programmes will equip students with a sound understanding of risk and with the knowledge and skills necessary to make safe and informed decisions.

All adults have a duty to keep children safe and protect them from radicalisation (Prevent Duty). The Trust forbids the promotion of partisan political views in the teaching of any subject.

Staff must:

- Ensure that they act appropriately in terms of their political behaviour, the views they express, and the use of school resources should not be used for party political purposes.

14. Monitoring Arrangements

This policy will be reviewed every year but can be revised as needed in line with any changing legislation. It will be ratified by the Trust Board.

Code of Conduct for Working with Children Policy Version 7 agreed at Trust Board

10 December 2025

Appendix A

Acceptable Usage agreement:

Partnership Trust – Staff

This agreement is for Staff, support staff, governors, visitors, wider stakeholders with access and external contractors.

When using the Trust ICT systems and accessing the internet, or offsite on a work device:

- I will not access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature.
- I will not use them in any way which could harm the school's reputation.
- I will not access social networking sites or chat rooms unless for educational purposes.
- I will not attempt to bypass the internet filtering or Trust/School IT security.
- I will not use any improper language when communicating online, including in emails or other communication systems.
- I will only use Trust IT systems, external logins, and email for school related purposes. Other use will be with the permission of Trust ICT Department.
- I will not divulge any Trust or School related passwords, and I will comply with IT security procedures.
- I will make sure email and social media interactions with staff, parents, students, and members of the public are responsible and in line with the Social Media, Safeguarding and Internet Safety policies.
- I will not give my home address, phone number, mobile number, personal social networking details or email address to students or parents.
- I accept that students and parents may find these details out, and that any contact should be logged and either not reciprocated or replied to in line with Trust policies.
- I will use Trust/School email systems for school and Trust related communications.
- I will not use personal accounts for Trust or school business.
- I will ensure that personal data is stored securely and in line with the Data Protection Policy.
- I will follow Trust/school policy regarding external logins, encrypted data and not storing school material on personal IT equipment.
- I will not install software onto workstations. Any software requests will be made to the Trust IT Department.
- I will not search for, view, download, upload or transmit any material which could be considered illegal, offensive, defamatory, or copyright infringing.
- Photographs of staff, students and any other members of the school and Trust community will not be used outside of Trust/School systems unless written permission has been granted by the subject of the photograph or their parent/guardian (where the subject is below the age of 18).
- I will ask the permission of the Head Teacher/Principal (on site) or the proprietor of the building (off site) prior to taking any photographs.
- I am aware that all network and internet activity is logged and monitored and that the logs will be made available to Trust Leaders or School Senior Leaders in the event of allegations of misconduct.
- I will comply with the social media policy.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the Data Protection Policy.
- I will inform the designated safeguarding lead (DSL) and Trust ICT manager if a student informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will champion the Internet Safety Policy and be a role model for positive and responsible behaviour on the school network and the Internet.

1. Data Protection and GDPR

The Data Protection Act 2018 and the GDPR legislation effective from 25th May 2018 states that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency').
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes ('purpose limitation').
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices that are owned by the school or Trust, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data.
- Transfer data using appropriately encrypted and secure means.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- This is only done for specific purposes with regards to providing these to a 3rd party where we have performed a Data Protection Impact Assessment (DPIA) and a formal agreement in place (for instance examination boards).
- You should never physically transport personal data for other purposes where you can digitally share the data within our pre-existing systems (for example OneDrive or SharePoint).
- the data must be encrypted, and password protected.
- When storing on a portable device the device must be owned by The Trust or School and must be secured by the ICT Department including a password and encryption.
- Data on removable media must be password protected (many memory sticks / cards and other mobile devices cannot be password protected, if this is the case then each individual file will need to be password protected).
- the data must be securely deleted from the device once it is no longer required.

Signed:

Date:

Employed at School: