HEARTS ACADEMY TRUST

Code of Conduct Policy 2023/2024

This policy will be reviewed annually on or before 1st September each year
Revised March 2024 - Prevent

HEARTS Academy Trust is committed to providing a happy, caring and safe learning environment for all within a values led context, where everyone feels valued and grows in confidence and independence.

We promote **HAPPINESS** through a creative, exciting and practical curriculum, which generates a love of, and interest in, learning and a resilience and hope which supports us through challenging times.

Great value is placed on pupils' self **ESTEEM** which is developed through a positive and motivated attitude to learning, a healthy lifestyle, good social skills, self-discipline and a positive self-image.

We promote the highest standards of **ACHIEVEMENT** in all areas of the curriculum and help all pupils to fulfil their potential regardless of gender, race or ability.

We foster **RESPECT and RESPONSIBILITY** for all by establishing good relations between the school, home and community. Pupils are taught respect for themselves, others and the environment. They are also taught to take full responsibility for their own choices and responsibility for themselves and their community.

We encourage **TRUTH** and honesty in all aspects of school life – relationships, work and the curriculum and learn to trust and accept others' individuality and uniqueness.

We develop **SPIRITUALITY and SERVICE** so that calm, quiet, reflective times which support deep thought are part of school life and beauty is appreciated. We promote a service culture that reflects our duty to support and show compassion to all members of the community and not just ourselves.

Children at the HEART

Contents

1. Introduction

The overriding expectation is that employees, volunteers, hirers and those engaged to work in the trust will adopt the highest standards of personal integrity and conduct both in and outside work. As role models they must behave, through their words and actions, at all times in a manner which demonstrates their suitability to work with children and which upholds the standards and reputation of the trust.

It is expected that hirers of school facilities will have appropriate safeguarding and child protection policies and procedures in place. Failure to have these in place will result in the termination of the agreement. Hirers should read the trust Letting policy in full.

This code of conduct provides an overall framework of the behaviours expected of individuals who work in the trust, whether as an employee, agency staff or a volunteer. The code is not intended to be exhaustive and individuals should use sound professional, ethical and moral judgement to act in the best interests of the trust, its pupils and its community.

At HEARTS, we are committed to safeguarding children and young people and we expect everyone who works in our school to share this commitment. We will always act in the best interest of the child.

As part of our continued commitment to safeguarding children, we require all adults who work for or with HEARTS Academy Trust, to provide accurate and up-to-date information as and when required. This may include, but is not limited to, DBS application; change of address details; notification of change of circumstances that may impact your ability to fulfil contractual duties etc.. Failure to do so may result in disciplinary action being taken and or costs being passed on to you via our payroll system.

This Code does not form part of any employee's contract of employment and it may be amended at any time.
The Code should be read in conjunction with:

- other trust policies and procedures;
- the terms of any employment or service contacts and agreements;
- relevant professional standards;
- Keeping Children Safe in Education;
- the HEARTS values which form the basis of our aims for pupils, staff, volunteers and governance.

2. Scope

This code applies to all employees regardless of length of service including those in their probation period.

The code also applies to consultants, contractors, casual and agency staff, volunteers, third-party workers, (collectively referred to as staff/workers in this policy). individuals); and voluntary workers.

As recognisable figures in the local community the behaviour and conduct of staff of the HEARTS Academy Trust outside of work can impact on their employment. Therefore, conduct outside work may be treated as a disciplinary matter if it is considered that it is relevant to the employees' employment (section 5.2 of this policy)

3. Roles and responsibilities

Trustees

It is the responsibility of the trustees to establish and monitor standards of conduct and behaviour within the trust, including the establishment of relevant policies and procedures.

Local advisory board members, trustees and members are subject to their own code of conduct.

Heads of Schools and Line Managers

It is the responsibility of heads of schools and line managers to address promptly any breaches of good conduct and behaviour, using informal procedures where possible but implementing formal procedures where necessary.

Employees
It is the responsibility of all employees to familiarise themselves with, and comply with, this code.

Any breaches of this code of conduct will be regarded as a serious matter which could result in disciplinary action, and in certain circumstances could lead to dismissal.

Engaged workers/volunteers, third-party workers and contractors
Engaged workers, third-party workers, contractors and volunteers are required to familiarise themselves and comply, with this code in so far as it is relevant to their role. Any breaches of this code may result in the engagement of the worker/volunteer being terminated, in accordance with any applicable terms of engagement.

4. Safeguarding and promoting the welfare of children and recognising low-level concerns - Reporting breaches of standards of good conduct

4.1 Low-level concerns about staff behaviour

The Trust wishes to promote an open environment that enables individuals to raise issues in a constructive way and with confidence that they will be acted upon appropriately without fear of recrimination.

All school-based employees, engaged workers, contractors, third-party workers and volunteers are responsible for safeguarding children and promoting their welfare. This means that all "workers" are expected to bring to the attention of a Head of School (deputy designated safeguarding lead for the trust, in the case of central staff, the CEO in the case of the deputy CEO and chair of trustees in the case of the CEO) any suspected concerns around the safeguarding of pupils or any breaches of our trust policies.

Any concerns around a Head of School should be reported to the Executive Headteacher.

Where appropriate, individuals should also refer to the trust's Whistleblowing Policy which is available from the school office and on the website.

5. The Code of Conduct

5.1 Safeguarding and Child Protection

It is essential that all adults working with children understand that the nature of their work and the responsibilities related to it, place them in a position of trust. Adults must be clear about appropriate and safe behaviours for working with children in paid or unpaid capacities, in all settings and in all contexts, including outside work.

The relevant requirements specific to safeguarding and child protection are set out in our:

- Child Protection policy
- Harmful Sexual Behaviour/Child on Child Abuse Policy;
- Behaviour, Anti-bullying and Exclusion policy;
- DfE Statutory Guidance "Keeping Children Safe in Education" (September 2023, as amended from time to time). This is the key statutory guidance which all employees must follow and all employees and volunteers must, as a minimum, read Part 1 and Annexe A of that Document.

5.1.1 Concerns about staff behaviour

Concerns may come from various sources, for example, a suspicion; complaint; or disclosure made by a child, parent or other adult within or outside of the organisation; or as a result of vetting checks undertaken.

The head of school/appropriate manager has to decide whether the concern is an allegation or low-level concern. The term 'low-level' concern does not mean that it is insignificant, it means that the behaviour towards a child does not meet the threshold for referral to the Local Authority Designated Officer (LADO) (see below).

5.1.2 Allegations

The guidance in KCSIE (Part Four) should be followed where it is alleged that anyone working in the school or college that provides education for children under 18 years of age, including supply teachers and volunteers has:

- behaved in a way that has harmed a child, or may have harmed a child;
- possibly committed a criminal offence against or related to a child;
- behaved towards a child or children in a way that indicates he or she may pose a risk of harm to children; or
- behaved or may have behaved in a way that indicates they may not be suitable to work with children.

5.1.3 Low-level Concerns

Concerns may be graded low-level if the concern does not meet the criteria for an allegation; and the person (could be anyone working in the organisation that provides education for children under 18 years of age, including supply teachers, volunteers and contractors) has acted in a way that is inconsistent with the expectations of this policy, including inappropriate conduct outside of work.

Low-level concern behaviours include, but are not limited to:

- being over-friendly with children;
- having favourites;
- taking photographs of children on their mobile phone;
- engaging with a child on a one-to-one basis in a secluded area or behind a closed door; or,
- using inappropriate sexualised, intimidating or offensive language.

To do this, employees must have fully read and understood our Child Protection and safeguarding suite of policies, be aware of our systems for keeping children safe and must follow the guidance in these polices at all times.

All employees must cooperate with colleagues and with external agencies where necessary.

If the concern has been raised via a third party, the head of school/appropriate manager will collect as much evidence as possible by speaking:

- directly to the person who raised the concern, unless it has been raised anonymously;
- to the individual involved and any witnesses.

Reports about supply staff and contractors should be notified to their employers, so any potential patterns of inappropriate behaviour can be identified.

Staff should be encouraged and feel confident to self-refer, where, for example, they have found themselves in a situation which could be misinterpreted, might appear compromising to others, and/or on reflection they believe they have behaved in such a way that they consider falls below the expected professional standards.

Low-level concerns should be recorded in writing, including:

- name* of individual sharing their concerns
- details of the concern
- context in which the concern arose
- action taken

(* if the individual wishes to remain anonymous then that should be respected as far as reasonably possible)

Records must be kept confidential, held securely and comply with the Data Protection Act 2018. HEARTS will retain such information in line with the Retention Schedule.

Records should be reviewed so that potential patterns of concerning, problematic or inappropriate behaviour can be identified.

If a concerning pattern of behaviour is identified and now meets the criteria for an allegation, then the matter should be referred to the LADO.

Individuals should familiarise themselves with these documents, in conjunction with the body of the Code of Conduct and other relevant trust policies and procedures.
In addition, individuals should be aware that it is criminal offence (s 16. Sexual Offences Act 2003) for a person aged 18 or over to have a sexual relationship with a child under 18 where that person is in a position of trust in respect of that child, even if the relationship is consensual.

Workers must not engage in any sexual activity within the school building or grounds at any time (with the exception of staff who live on site, within their own living quarters) or whilst engaged in school business.

5.1.4 Prevent
From July 2015 all schools (as well as other organisations) have a duty to safeguard children from radicalisation and extremism. This means we have a responsibility to protect children from extremist and violent views the same way we protect them from any other harm. Importantly, we can provide a safe place for pupils to discuss these issues, at an appropriate level so they better understand how to protect themselves.

Many of the things we already do in school to help children become positive, happy members of society also contribute to the Prevent strategy. These include:

- Focusing on the core HEARTS values, the ethos that pervades our school
- Exploring other cultures and religions and promoting diversity
- Challenging prejudices and racist comments
- Developing critical thinking skills and a strong, positive self-identity
- Promoting the spiritual, moral, social and cultural development of pupils, as well as British values such as democracy

Read in conjunction with the Trust Child Protection and Online Safety Policies, individual school Prevent risk assessments and statement.

5.2 Conduct outside work
The Trust recognises and respects individuals' right to a private life without interference. However, individuals connected with the trust must not act in a way that would bring the school, trust or their profession, into disrepute or that calls into question their suitability to work with children. This covers relevant criminal offences, such as violence or sexual misconduct, inappropriate behaviour such as lewd or offensive action, as well as negative comments about the school, trust or its community. This includes posting, sharing or liking sexually offensive, racist, homophobic, transphobic or sexist content with electronic devices, on social media or other sites. Employment outside school that might bring the trust into disrepute including prostitution, sex chat lines, naked modelling, criminal activity involving cruelty to animals and extremist activity is not permitted.

When workers are attending educational visits, residential visits, training courses or international visits, their behaviour must reflect this code of conduct at all times.

Employees are required to demonstrate responsible behaviour at work-related functions and work-related social events that take place outside normal working hours and to act in a way that will not have a detrimental effect on the reputation of the trust.

Workers must disclose to the school, in writing and immediately (Head of School/Executive Headteacher or Chair of Trustees) any wrongdoing or alleged wrongdoing by themselves (regardless of whether they deny the wrongdoing/alleged wrongdoing), including any incidents arising from alternative employment or outside of work which may have a bearing on their employment or engagement with the trust.

Employees should also refer to the expectations set out in their contract of employment and the disciplinary procedures.

In addition, any worker engaged in a post covered by the Childcare (Disqualification) Regulations 2006 ("the

Regulations") must immediately inform the trust of any events or circumstances which may lead to their disqualification from working in the post by virtue of the Regulations. The statutory guidance relating to Childcare (Disqualification) and Childcare (Early Years Provision Free of Charge) (Extended Entitlement) (Amendment) Regulations 2018 ("the 2018 regulations") Disqualification under the Childcare Act 2006/regulations 2018 can be found in the following link: Disqualification under the Childcare Act 2006.

5.2.1 Secondary employment

The trust does not seek to unreasonably preclude employees from undertaking additional employment but employees are required to devote their attention and abilities to their duties at the trust during their working hours and to act in the best interests of the trust at all times. Any additional employment must be discussed with the Head of School/Executive Head. The trust also has a duty to protect health and safety in relation to an employee's working hours. Accordingly, employees must not, without the written consent of the trust, undertake any employment or engagement which might interfere with the performance of their duties. In addition, employees should avoid engaging in business or employment activities that might conflict with the trust's interests.

5.3 Confidentiality and data protection

Members of staff may have access to confidential information about pupils, colleagues or other matters relating to HEARTS Academy Trust. This could include personal and sensitive data, for example information about a student's home life. Employees should never use this information to their own personal advantage, or to humiliate, intimidate or embarrass others. Employees should never disclose this information unless this is in the proper circumstances and with the proper authority.
If an employee is ever in doubt about what information can or can't be disclosed they should speak to the trust Data Protection Officer (DPO)

We will comply with the requirements of Data Protection Legislation (being the UK General Data Protection Regulation and Data Protection Act 2018) and any implementing laws, regulations and secondary legislation, as amended or updated from time to time. Employees are expected to comply with the trust's systems as set out in our Data Protection Policy. If any employee becomes aware that data is at risk of compromise or loss, or has been compromised or lost they must report it immediately to the Data Protection Officer, in order (where applicable) for relevant breaches to be reported to the Information Commissioners Office within 72 hours.

Employees must read and understand our Data Protection Policy and other relevant policies including in relation to criminal records information, recruitment and safer recruitment, internet, email and communications, information security, copies of which are available on the trust website and from the school office.

When an employee leaves the trust they are not permitted to take any data or information with them without explicit written consent from the CEO or Deputy-CEO.

5.3.1 Preserving anonymity

The Education Act 2011 contains reporting restrictions preventing the publication of any material which could lead to the identification of a teacher in the event of an allegation against them made by a pupil at the same school. Any individual who publishes material which could lead to the identification of the employee who is the subject of an allegation of this kind may be subject to criminal and disciplinary action, up to and including dismissal.

"Publication" includes any speech, writing, relevant programme or other communication in whatever form, which is addressed to the public at large or any section of the public. For the avoidance of doubt, this includes publishing details of an allegation or other information on a social media site which could lead to the identification of the teacher. Enquiries from official authorities, e.g. police or social care, must be referred to the Executive Headteacher as they are the only level of management authorised to speak on these matters.

5.3.2 Media queries

Workers must not speak to the press or respond to media queries on any matter relating to the school or trust. All media queries should be referred immediately to the Chief Operating Officer (COO) or Trust Business Manager (TBM).

5.4 Use of computers, email and the internet and social media

The trust recognises that electronic devices and media are important tools and resources in an educational context and can save time and expense.

Those using the trust's equipment and networks are expected to do so responsibly and to comply with all applicable laws, policies and procedures, to include GDPR, Cyber Security and with normal standards of professional and personal courtesy and conduct.

Personal use of social media and other on-line applications which may fall into the public domain should not be such that it could bring the school or trust into disrepute and/or call into question an individual's suitability to work with children.

An email good practice guide can be found at Appendix C.
The acceptable Use of ICT Agreement can be found at Appendix D including expectation when using Teams

Any worker who is unsure about whether or not something he/she proposes to do might breach that policy or if something is not specifically covered in the policy they should seek advice from their line manager or a member of the senior leadership team.

Staff members/trustees/LAB members/volunteers will not name pupils, other staff or their place of work on their personal email/social media accounts.

Work devices including computers, tablets, laptops, mobile phones etc. should be used for work related messaging only and not for personal communication.

Staff must not use personal electronic communication devices such as mobile phones or iPads as cameras in school. Any photographs/video footage must be taken using school equipment. Staff must only save images on school IT hardware/computers.

Staff who are in contact with pupils should not use personal mobile phones in school during their directed/paid hours of employment unless there are exceptional circumstances and they have requested and been given explicit permission to do so by the principal/ headteacher. Outside of these times, mobile phones should only be used in areas of the school where pupils are not present.

The trust has implemented protective measures to limit risks. All staff are expected to follow Multi-Function Authenticator (MFA) procedures to access HEARTS emails, financial platforms and web-based systems.

Photography, videos and other images/media

Many educational activities involve recording images. These may be undertaken, with parental permission, for displays, publicity, to celebrate achievement and to provide records of evidence of the activity. Under no circumstances should employees use their personal equipment to take images of pupils at or on behalf of the Trust.

5.5 Relationships

5.5.1 The internal school and trust community

All workers are expected to treat members of the school and trust community with dignity and respect and to work co-operatively and supportively. Bullying, harassment and victimisation will not be tolerated (see also the trust's grievance procedure and the HEARTS values)

5.5.2 The wider community and service users

All workers have a responsibility to ensure courteous, efficient and impartial service delivery to all groups and

individuals within the community. No favour must be shown to any individual or group of individuals, nor any individual or group unreasonably excluded from, or discriminated against, in any aspect of trust business.

5.5.3 Contracts

All relationships of a business or private nature with external contractors, or potential contractors, must be made known to board of trustees. Orders and contracts must be in accordance with the financial regulations of the trust. No special favour should be shown to businesses run by, for example, friends, partners or relatives in the awarding of contracts, tendering process or any other business transaction. A declaration / conflicts of interest from should be completed when any business is transacted with close contacts.

5.5.4 Gifts and Hospitality

Workers may not accept any gift or hospitality from a person intended to benefit from their services (or those whom they supervise) or from any relative without the express permission of the trust.

Where an outside organisation wishes to sponsor or is seeking to sponsor a school activity, whether by invitation, tender, negotiation or voluntarily, the sponsorship should always be related to the school's interests and never for personal benefit.

The trust's policy on gifts and hospitality is available from the school office and the trust website. Any breaches of this policy may lead to disciplinary action.
For many of our employees there will be a limited opportunity to accept gifts and hospitality, but all staff must be aware that it is not acceptable for staff to accept bribes. Therefore, any gift, promotional offer or hospitality, intended either for the employee or for the school that exceeds a nominal value of £25.00 must be declared to the School Business Manager within 5 working days and permission must be obtained before accepting. If an employee is ever unsure, then the best course of action is to politely decline the offer.

The above is also applicable for the traditional of pupils and their parents or carers to give gifts as a small token of appreciation or as a thank you to members of staff at certain times throughout the academic year. This Code of Conduct is not designed to stop that practice. Staff may accept gifts from pupils and their parents or carers provided that they meet this definition and as set out above, any gifts over the value of £25.00 must be reported to the School Business Manager. Staff should make the Headteacher aware of any pupil/parent who is giving them gifts on a regular basis, or any pupil or parent or carer who expects something in return for a gift, as this would not be acceptable.

5.5.5 Neutrality

Workers must not allow their own personal, political, religious or other views and opinions to interfere with their work. They are expected to be neutral in their views in the course of their work at the trust and to present a balanced view when working with pupils.

5.6 Close personal relationships at work

Close personal relationships are defined as:

- workers who are married, dating or in a partnership or co-habiting arrangement;
- immediate family members for example parent, child, sibling, grandparent;
- other relationships for example extended family (cousins, uncles, in-laws), close friendships, business associates (outside the trust).
- Sexual relationships however brief. This includes, but not exclusively, sexting, intimate kissing, sexual intercourse, oral sex, mutual masturbation, sexual play and other penetrative or non-penetrative acts.

5.6.1 Relationships at work

It is also recognised that situations arise where close personal relationships can be formed at work. Such relationships should be disclosed, in confidence, to the line manager by the individuals concerned as this may impact on the conduct of the trust.

Whilst not all such situations where those in close personal relationships work together raise issues of conflict of interest, implications can include:

- effect on trust and confidence;
- perception of service users, the public and other employees on professionalism and fairness;
- operational issues e.g. working patterns, financial and procurement separation requirements;
- conflicting loyalties and breaches of confidentiality and trust.

Open, constructive and confidential discussion between workers and managers is essential to ensure these implications do not occur and that all parties can be protected.

No-one should be involved in discipline, promotion, pay or other decisions for anyone where there is a close personal relationship.

It may be necessary in certain circumstances to consider transferring workers that form close personal relationships at work. Any such action will be taken wherever possible by agreement with both parties and without discrimination. Staff will not be line managed by family members or by someone with whom they have a close personal relationship.

Colleagues who feel they are affected by a close personal relationship at work involving other colleagues should at all times feel that they can discuss this, without prejudice, with their head of school/line manager, other manager or Chair of Trustees.

5.6.2 Workers related to pupils

Any workers related to, or who are the carer of a pupil, are expected to separate their familial and employment role.

Workers must not show or provide any preferential treatment to them or become involved in their education or care beyond their specific role as an employee/volunteer or their role as a parent/carer/relation.

5.6.3 Applicants

Applicants are required to disclose on their application form if they have a close personal relationship with any person connected with the trust.

Applicants are asked to state the name of the person and the relationship. Failure to disclose such a relationship may disqualify the applicant.

Workers should discuss confidentially with their head of school/line manager, any relationships with an applicant.

It is inappropriate for any worker to sit on a shortlisting, interview or appointment panel, for those with whom they have a close personal relationship.

5.6.4 References

The purpose of seeking/providing references is to allow the sharing of factual information to support appointment decisions. It is expected that, for those working with children, professional references, and not personal references, are sought and provided. All references provided on behalf of the school or trust must be signed by the Head of School (Executive Headteacher for the Head of School, CEO for the Executive Headteachers and Chair of trustees for CEO).

Anyone agreeing to act as a personal referee must make it clear in the reference that it is provided as a personal or colleague reference, use their own address and make no reference to the school, trust or their employment. Personal or colleague references must not be provided on school or trust-headed paper.

5.7 Dress code
The dress code for staff is found in Appendix E.

5.8 Use of financial resources
Workers must ensure that they use public and any other funds entrusted to them in a responsible and lawful manner. They must strive to ensure value for money and ensure rigorous adherence to Financial Regulations.

5.9 School/Trust Property and personal possessions
Workers must ensure they take due care of school and trust property at all times, including proper and safe use, security, appropriate maintenance and reporting faults and the use of MFA as detailed under section 5.4 of this code. If employees are found to have caused damage to the school or trust property through misuse or carelessness this may result in disciplinary action.

Permission to take, use or access trust property, including emails and website platforms, outside of the UK must be sought in writing from the Executive Headteacher.

Workers are responsible for the safety and security of their personal possessions while on trust premises. The trust will not accept responsibility for the loss or damage of personal possessions.

6.0 Behaviour

6.1 Use of language
”Workers” should not use any form of degrading or humiliating treatment to punish a student. The use of sarcasm, demeaning or insensitive comments towards pupils or colleagues is completely unacceptable.
All “workers” must:

- avoid words or expressions that have any unnecessary sexual content or innuendo;
- not use language that could be considered racist, sexist or homophobic;
- not use language that promotes extreme political ideas or that promotes any form of radicalisation;
- avoid any words or actions that are over-familiar;
- not swear, blaspheme or use any sort of offensive language in front of pupils;
- understand that the use of sarcasm or derogatory words should be avoided when implementing behaviour management and unprofessional comments about anyone must also be avoided;
- take care if engaging in banter with pupils and/or colleagues, however well intended.

6.2 Smoking
All trust premises are non-smoking sites and workers must observe this.

6.3 Alcohol and Substance misuse
“Workers” are expected to arrive at work fit to carry out their job and to be able to perform their duties safely without any limitations due to the use or after effects of alcohol or drugs. In this policy drug use includes the use of controlled drugs, psychoactive (or mind-altering) substances formerly known as "legal highs", and the misuse of prescribed or over-the-counter medication.

Alcohol and drug-related problems may develop for a variety of reasons and over a considerable period of time. Therefore, HEARTS Academy Trust will seek, where appropriate, to treat these problems in a similar way to other health issues. Support may be provided at this point, in order to aid a full recovery, allowing a return to work/effective performance and the full range of duties.

Staff must not drink alcohol during the normal school working day nor should they drink alcohol with pupils outside of the normal working day. The consumption of alcohol on all trips involving children is not permitted. Drivers

must not consume alcohol under any circumstances. It is a disciplinary offence to be on school premises and/or carrying out official duties when under the influence of non-medically prescribed drugs and/or alcohol.

All staff medication must be kept locked away or left in a vehicle at all times. If you are taking long-term medication, this should be declared to your line manager. Appropriate measures and risk assessments will be put in place to support you should this be necessary.

6.4 Gambling

Gambling activities must not be conducted on trust premises; discretion may be used in relation to small raffles for charitable purposes, national lottery syndicates, occasional sweepstakes etc.

7. Social contact with pupils

7.1 Employees should not establish or seek to establish social contact, via any channels (including social media), with pupils or their parents for the purposes of securing a friendship or to pursue or strengthen a relationship. Employees should use their work provided equipment only for communicating electronically with pupils. Workers must not provide their personal contact details, including phone numbers, email address etc, to any pupil or their parent.

Workers should not connect to pupils or their parents via social media or other communication channels.

Our schools are part of local communities and we recognise that, as members of the community, employees will come into contact with pupils outside of the school. We expect staff to use their professional judgement in such situations and to report to the Head of school any contact that they have had with a student, outside of school, that they are concerned about or that could be misinterpreted by others.

7.2 Social Media

Staff must not post disparaging or defamatory statements about our school's or trust, our pupils or their parents or carers; our governors or staff; suppliers and vendors; and other affiliates and stakeholders. Staff should avoid social media communications that might be misconstrued in a way that could damage our trusts reputation, even indirectly. If you see content in social media that disparages or reflects poorly on our trust or our stakeholders, you should print out the content and contact the Head of School. All workers are responsible for protecting our trust's reputation.

8. Keeping within the law

8.1 Staff are expected to operate within the law. Unlawful or criminal behaviour, at work or outside work, may lead to disciplinary action, including dismissal, being taken. However, being investigated by the police, receiving a caution or being charged will not automatically mean that an employee's employment is at risk.

8.2 Employees must ensure that they:

8.2.1 Uphold the law at work

8.2.2 Never commit a crime away from work which could damage public confidence in them or the trust, or which makes them unsuitable for the work they do. This includes, for example:

- submitting false or fraudulent claims to public bodies (for example, income support, housing or other benefit claims)
- breaching copyright on computer software or published documents
- sexual offences which will render them unfit to work with children or vulnerable adults
- crimes of dishonesty which render them unfit to hold a position of trust.

8.2.3 Write and tell the Head of School (CEO and Deputy-CEO if they are the Head of School, Chair of Trustees if they are the CEO or Deputy CEO) immediately if they are questioned by the police, charged with, or convicted of, any crime whilst they are employed at the trust (this includes outside of their working hours). The Head of School and/or Trustees will then need to consider whether this charge or conviction damages public confidence in the trust or makes the employee unsuitable to carry out their duties.

9. Agency workers

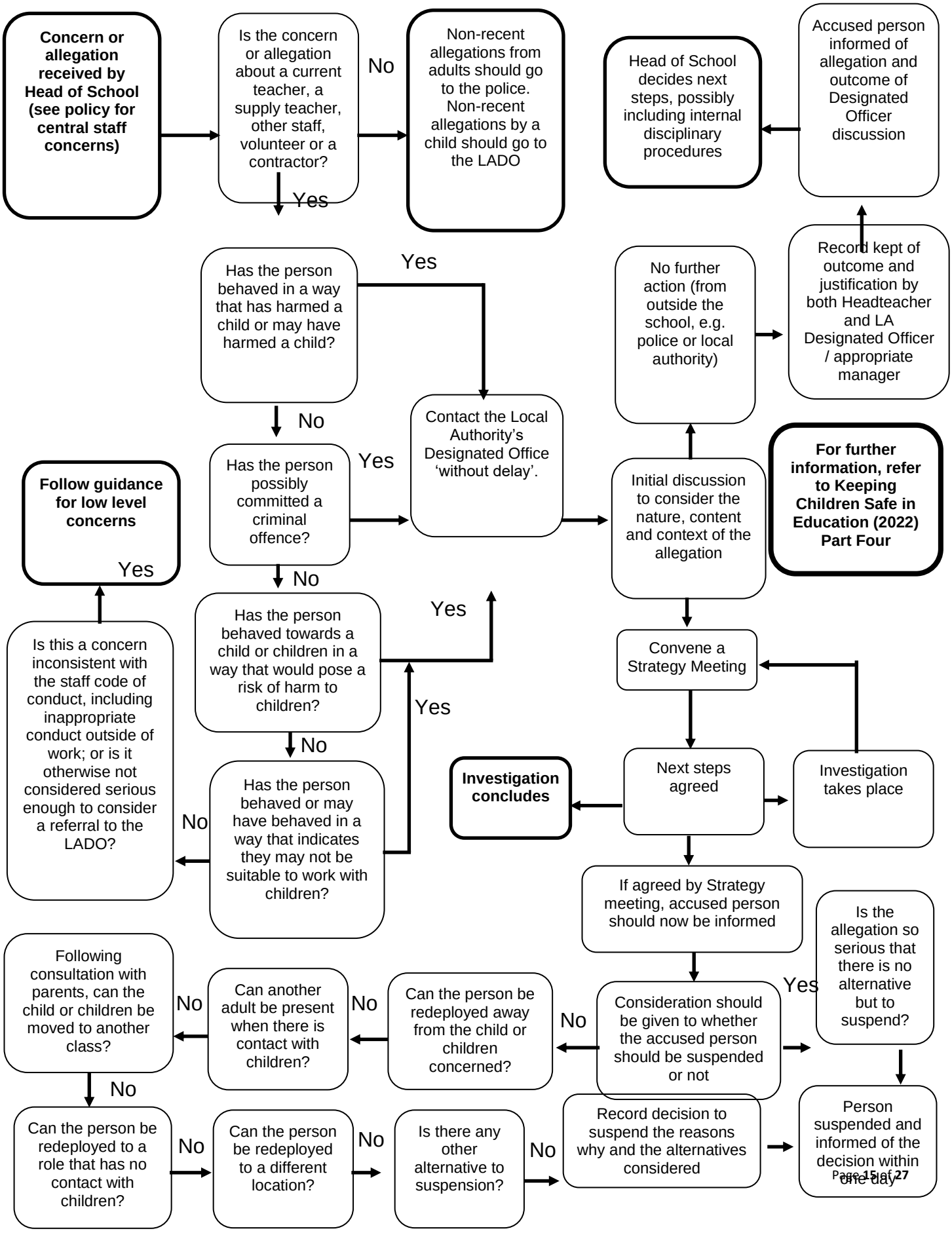
9.1 We will investigate allegations made against agency workers with the cooperation of the agency. Whilst we may decide to cease using the services of an agency worker, this will not prevent us from investigating allegations and liaising with the Local Authority Designated Officer (LADO) to determine a suitable outcome. We expect agency workers and agencies to cooperate with our investigations and with external agencies where applicable.

9.2 We will discuss with the agency whether it may be appropriate for them to consider suspending an agency worker, or whether we are prepared to redeploy an agency worker during an investigation.

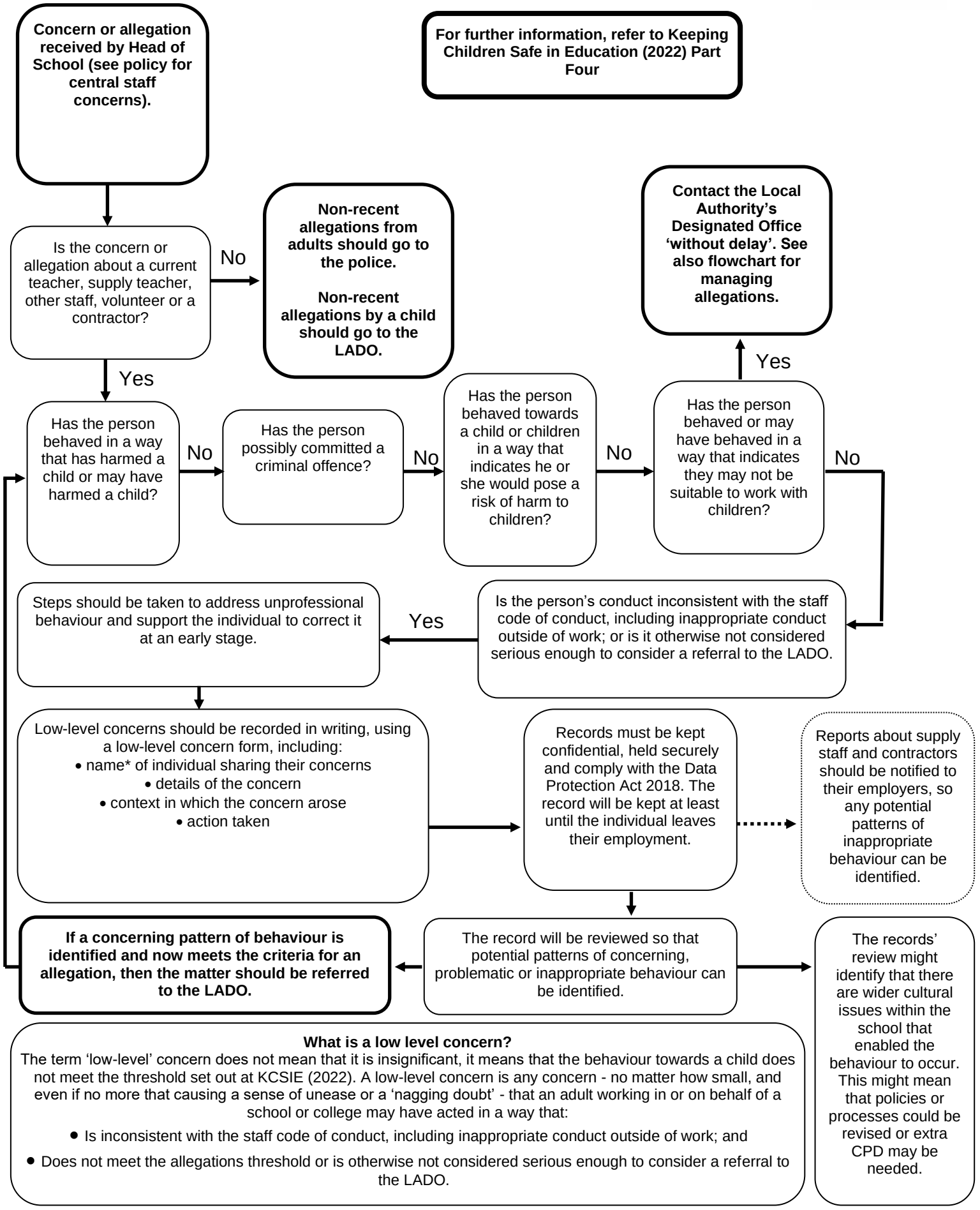
10 Review

This Code of Conduct is reviewed and amended annually by the trust. We will monitor the application and outcomes of this code of conduct to ensure it is working effectively.

Appendix A—Allegations made against / concerns raised in relation to teachers, including supply teachers, other staff, volunteers (Andrew Hall 2021)



Appendix B - Managing low level concerns raised in relation to teachers, including supply teachers, other staff, volunteers and contractors (Andrew Hall 2021)



What is a low level concern?

The term 'low-level' concern does not mean that it is insignificant, it means that the behaviour towards a child does not meet the threshold set out at KCSIE (2022). A low-level concern is any concern - no matter how small, and even if no more that causing a sense of unease or a 'nagging doubt' - that an adult working in or on behalf of a school or college may have acted in a way that:

- Is inconsistent with the staff code of conduct, including inappropriate conduct outside of work; and
- Does not meet the allegations threshold or is otherwise not considered serious enough to consider a referral to the LADO.

Appendix C - Email Good Practice Guide

Good Practice	
Read receipt	When it is important to know that a recipient has opened a message, it is recommended that the sender invoke the 'read receipt' option.
Attachment formats	When attaching a file, it will have a specific format. Be aware of the possibility that a recipient may not have the software necessary to read the attachment. Format incompatibility can occur even between successive versions of the same software, e.g., different version of Microsoft Word.
Message header, or subject	Convey as much information as possible within the size limitation. This will help those who get a lot of e-mails to decide which are most important, or to spot one they are waiting for.
Subject	Avoid sending messages dealing with more than one subject. These are difficult to give a meaningful subject heading to, difficult for the recipient to forward on to others for action, and difficult to archive.
Recipients	Beware of sending messages to too many recipients at once. When sending messages for more than one-person's use be sure to indicate people for whom there is some expectation of action or who have central interest. cc to indicate those who have peripheral interest and who are not expected to take action or respond unless they wish to do so.
Replying	When replying to a message sent to more than one person, do not reply to all recipients of the original message, unless you are in leadership or you have been requested to do so. Consider who needs to read your reply, e.g. if the sender is organising a meeting and asking you for availability dates, you need only reply to the sender. One drive settings should be set to default to reply.
Holiday closures/absences	When absent due to sickness, agreed leave or holiday closures set the 'out of office' message. You won't lose your messages, they will await your return, but the sender will know that you're not there and can take alternative action if necessary.
Evidential record	Never forget that electronic conversations can produce an evidential record which is absent in a telephone conversation. Comments made by an employee during the course of an exchange of e-mails could be used in support, or in defence, of the school's legal position in the event of a dispute.
Legal records	Computer-generated information can now be used in evidence in the courts. Conversations conducted over e-mail can result in legally binding contracts being put into place.
E-Mail threads	Include the previous message when making a reply. This is called a thread. Threads are a series of responses to an original message. It is best that a response to a message is continued by using reply accessed on the quick menu bar, rather than start an entirely new message for a response. Keep the thread information together. It is easier for the participants to follow the chain of information already exchanged. If the message gets too long the previous parts can be edited while still leaving the essence of the message. The use of threads is to be used when there is just one subject, to avoid the accidental disclosure of information to the incorrect person.
Context	E-mail in the right context, care should be taken to use e-mail where appropriate. There may be occasions when a telephone call would be more appropriate especially on delicate matters. Beware of the use of excessive use of capitals. It can be interpreted as shouting so consider how the style of your email may be interpreted by its recipient.

Forwarding e-mails	Consideration should be given when forwarding e-mails that it may contain information that you should consult with the originator before passing to someone else.
Large e-mails	For larger e-mails, particularly Internet e-mails, where possible send at the end of the day as they may cause queues to form and slow other people's e-mail.
Data protection	Emails with attachments that hold special information should have their attachments password protected. Telephone the recipient with the password. Always be aware that emails can be requested as part of a subject access request and should not include information that you are not happy to share with the subject. Emails about a pupil or staff member should refer to the pupil with initials or full name.

Appendix D – ICT Acceptable Use Agreement including the use of mobile devices

1. Introduction

ICT (including data) and the related technologies such as computers, email, the internet and mobile devices are an expected part of daily working life in school and the use of electronic communication and resources is encouraged.

This policy is designed to ensure that all staff are aware of their personal and professional responsibilities when using any form of ICT. All staff are expected to read and understand this policy

All members of the trust community are expected to use ICT responsibly and to comply with all applicable laws, policies and procedures, and with normal standards of professional and personal courtesy and conduct.

The Trust will take a wide and purposive approach to considering what falls within the meaning of technology. This policy relates to all technology, computing and communication devices, network hardware and software and services and applications associated with them including:

- The internet
- Email
- Mobile phones and smartphones
- Desktops, laptops, notebooks, tablets / phablets
- Personal music players (iPods or other devices)
- Devices with the capability for recording and/or storing still or moving images
- Social networking, blogging and other interactive web sites
- Instant messaging (including image and video messaging apps and other forms of social media, including WhatsApp), chat rooms, blogs and message boards
- Webcams and video hosting sites (such as YouTube)
- Gaming sites and online chats through gaming
- Virtual learning environments (the GSuite for Education: Google Classroom and Google Meet, Dojo, Tapestry etc)
- SMART boards
- Other photographic or electronic equipment, including wearable technology (smart watches)

Failure to follow this policy may result in the withdrawal of access to trust computers, email and internet and/or to disciplinary action, depending on the circumstances of the case.

Technology and the law change regularly and this policy will be updated as and when necessary. Workers will be informed when the policy has changed but it is their responsibility to read the latest version of this document.

It is the aim of The Trust to create highly skilled and independent users of technology. We want all staff to be digitally literate and able to navigate the online world with increasing skill, precision and efficiency while maintaining the utmost principles of online safety and safeguarding. We recognise that this is crucial to prepare learners for life in the modern world and for the next stage of their lives.

The Trust will support all staff to develop their skills whilst balancing the safety and welfare of pupils and the security of our systems. All pupils are educated, as part of our curriculum, about the importance of safe and responsible uses of technology and how to protect themselves (and others) online.

All staff are responsible for their actions, conduct and behaviour when using technology. The use of technology should be safe, responsible and respectful to others and at all times legal. Any misuse of technology by staff will be dealt with under the Discipline and Dismissal Procedure.

In any cases that give rise to safeguarding concerns, the matter(s) will be dealt with under our child protection procedures (following our Safeguarding and Child Protection policy). Matters will be dealt with by the DSL (or Head

of School in the case of concern about the conduct of a staff member) and recorded in line with our procedures and systems. In cases where the concern is related to the Head of School, this will be escalated to the Executive Head, concerns about Executive Head should go to the CEO (and concerns about the CEO should go to the Chair of Trustees. In the case of the central team, a concern must be reported to the Deputy Designated Safeguarding Lead (DDSL) for the Trust.

Training will be provided for all stakeholders on how to use and navigate our IT systems, particularly Google Classroom and Google Meet, by trained and competent school leaders. All stakeholders will feel confident to be able to safely deliver lessons and other educational content online when needed.

Please also refer to Keeping Children Safe in Education and our Child Protection Policy for additional information.

2. Use of School and trust equipment/networks

Computers, mobile phones and other devices provided by the trust are loaned to individuals to support their professional responsibilities and must be used in accordance with this policy.

Workers are responsible for the safe and proper use, care and security of equipment and systems provided. Devices must be secured appropriately especially when leaving the trust premises (i.e., not left unattended) and protected from unauthorised access or use (i.e. not accessed by family members). Any loss, damage or unauthorised access must be reported immediately.

Workers must not use trust equipment, networks or system to access, download, send or receive, store, create, copy or distribute any material which may be malicious, illegal, libellous, immoral, dangerous or offensive (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).

Any appropriate and authorised electronic communication with pupils must be through official trust networks, channels, systems and on trust equipment.

Permission to take, use or access trust property, including emails and website platforms, outside of the UK must be sought in writing from the Executive Headteacher.

3. Use of Email

Trust business must always be conducted through official email addresses, which must be secured with password controls. Workers should respond to emails during working hours in a timely and appropriate fashion. Occasionally a member of staff may choose to send emails outside of their normal working hours, but there is no obligation for emails received to be checked or responded to.

Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

Extreme care must be taken with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

Email must not be used to receive, send or forward messages that are defamatory, obscene or otherwise inappropriate. If such an email is received, whether unwittingly or otherwise and from whatever source, this must not be forwarded to any other address and must be reported immediately.

Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.

The trust has implemented protective measures to limit risks. All staff are expected to follow Multi-Function Authenticator (MFA) procedures to access HEARTS emails, financial platforms and web-based systems.

4. Social Networks

Social networking applications include but are not limited to:

- Blogs
- Online discussion forums, for example Facebook;
- Media sharing services for example YouTube;
- Professional networking sites, for example Linked In;
- 'Micro-blogging' application for example Twitter.

Where the school/trust operates official networking sites, these must be managed and used in accordance with this policy. This includes the following requirements:

- use of official (i.e. not personal) email addresses for user accounts;
- appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users;
- the school/trust logo and other branding elements should be used to indicate the school/trust support. The school/trust logo should not be used on social networking applications which are unrelated to or are not representative of the school/trust;
- users should identify themselves as their official position held within the school/trust on social networking applications e.g. through providing additional information on user profiles;
- any contributions on any social networking application must be professional, uphold the reputation of the school/trust and be in accordance with data protection requirements;
- users must not promote or comment on personal matters (including personal/ financial matters), commercial ventures, political matters or campaigns, religion or other matters;
- users should not respond to personal requests, abuse or questionable comments by parents or members of the public.

5. Personal use of trust equipment/networks

Trust equipment, internet services, systems and email may be used for incidental personal purposes, with the approval of the line manager, provided that it:

- does not interfere with the trust's operation of computing facilities or email services;
- does not interfere with the user's employment or performance of professional duties or other obligations to the trust;
- is of a reasonable duration and frequency;
- is carried out in authorised break times or outside their normal working hours;
- does not over burden the system or create any additional expense to the trust;
- is not used to access, send, receive or store inappropriate material; and
- does not bring the trust and its community into disrepute.

Workers must notify the trust of any significant personal use.

Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.

Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

Trust equipment/networks/systems must additionally not be used for

- commercial purposes not under the auspices of the trust;
- personal financial gain;
- personal use that is inconsistent of other trust policies or guidelines; or
- ordering of goods to be delivered to the school/trust address or in the school/trust's name.

6. Used of personal ICT equipment in school/trust

- Staff must secure their personal mobile phones and other devices during the school day in a locker or in a closed bag in a cupboard. All phones and other personal devices must be turned off during the school day.
- Telephones in the main school offices should be manned between 8.30am and 3.30pm so that urgent messages for staff can be passed on quickly.
- Mobile phones can be checked in the staff room at breaktime, lunchtime or after school.
- Once all children have left the building, staff can have mobile phones turned on and with them.
- All telephone contact with Parents/Carers from the school must be made on the school telephone and not on personal phones or from home.
- During group visits off the school site, staff may carry their own phones in bags but they should only be used in emergencies.
- All photographs of children taken in school must be deleted immediately after use unless they are being collected for strategic documents, in which case they should be forwarded to the office manager for secure storage.
- No parent is permitted to use their mobile phone whilst inside the school building or on the site. All devices should be turned off. Instructions about this will be given out at the start of school events with reminders as necessary.
- Visitors to the school must turn off their phones on entering the building. If a contractor requires an electronic device to work in school, then an appointment must be made in advance with an appropriate member of the office or site staff.
- There may an exception to the use of mobile phones in school in an emergency or for the continuation of business and this must be agreed and risk assessed by EHT/ HOS.

<u>Other electronic devices</u>
Workers should not bring other electronic devices onto school premises unless this has been specifically authorised by an appropriate manager. In such circumstances, the computer / equipment must be kept securely (at the risk of the owner) and security protected so that it cannot be accessed by pupils or others at the school.

Any personal use of such equipment must be restricted to an employee's break times or outside their normal working hours and must not impact on their duties in any way.

Additionally, specific permission must be obtained prior to connecting any device to school networks/systems and the device(s) must have adequate virus protection.

Workers must ensure that no personal information regarding school/trust business, its pupils or staff is stored on such personal equipment.

Where exceptionally, specific permission is granted to use personal equipment for work purposes e.g. to give a presentation, the employee must be extremely vigilant that personal files/data etc. are not inadvertently accessed or displayed.

No pictures or videos may be taken within school or at any school related activity, on personal devices.

It is acknowledged that Ofsted inspectors are permitted to use electronic devices in school for the purpose of their inspection of work.

7. Personal social networks

The trust recognises individual rights to privacy and a private life. However, the law generally views social media as in the public domain, irrespective of privacy settings. Workers are therefore advised to be mindful of their duties and obligations to uphold the reputation of the trust, to comply with the code of conduct and other policies and contractual terms in their use of personal social media – being mindful of the real possibility for material to be posted, shared and made public inadvertently or by other contacts.

The trust may require the removal of content it considers inappropriate.

It is totally unacceptable for any worker to discuss pupils, parents, work colleagues or any other member of the trust community or any trust related business on any type of social networking site.

Other posting/ liking or retweeting etc on personal sites may also impact on the reputation of the school/trust or the suitability/conduct of the employee, for example if an employee is off sick but makes comments on a site to the contrary, postings of indecent, racist, sexist, discriminatory or inappropriate images/activities etc.

Workers must not accept or propose contact, nor engage in any conversation with pupils on any personal social networking sites and should be circumspect in personal network contact with former pupils, particularly those under the age of 18 years.

Individuals working in the school should not use or access social networking sites of pupils.

Employees, volunteers, Trustees or LAB members should not name schools, the trust or pupils, parents, carers on social media sites.

8. Security

The trust follows sound professional practices to secure data, system programmes, email records and networks under its control.

Workers must take all reasonable precautions to maintain security and confidentiality and to protect data. This includes:

- using appropriate security measures such as encryption/password protection to transmit confidential or sensitive information;
- ensuring all devices and system access are password protected. (All laptops, memory sticks and devices used must be encrypted). Memory sticks containing data must not be removed from the trust premises;
- ensuring that pupils are not exposed to any inappropriate images or web links; and
- respecting all copyrights and not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Users must not:

- use, transfer or tamper with other people's accounts and files;
- use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system;
- store sensitive, confidential data or photos on their own equipment – this extends to personal cameras, mobile phones and other similar devices;
- use the internet/intranet facilities or equipment to deliberately create any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations.
- monitor or intercept the files or electronic communications of other workers or third parties;
- hack or obtain access to systems or accounts they are not authorised to use;
- use other people's log-ins or passwords; or
- breach, test, or monitor computer or network security measures without authorisation.

Where any security breach or inappropriate connection or ICT activity occurs, the user must immediately disconnect/log out and report immediately.

The trust has implemented protective measures to limit risks. All staff are expected to follow Multi-Function Authenticator (MFA) procedures to access HEARTS emails, financial platforms and web-based systems.

9. Privacy and Monitoring

The trust respects workers' privacy and will not routinely inspect or monitor emails, data or internet usage.

However, workers should not have any expectation of absolute privacy in his or her use of the trust systems or equipment (including but not limited to networks/servers/internet usage/networks/Wi-Fi). Under the following circumstances the trust reserves the right, at its discretion, to review any electronic files and messages to the extent necessary to ensure systems are being used appropriately:

- when required by law;
- if there is a substantiated reason to believe that a breach of the law; or trust policy has taken place;
- if the trust suspects that the employee has been viewing/transmitting offensive or illegal material;
- if the trust suspects that the employee has been spending an excessive amount of time on activity which is not work related;
- where required for compliance checks e.g. auditors, data protection; or
- where there are emergency or compelling circumstances such as staff absence

The trust will endeavour to notify affected individuals of any monitoring which will take place and the reason for it, save in exceptional circumstances (see below).

Workers will normally be notified of what information will be recorded and retained, and for how long, who will have access and how such information will be used, which will include using such information for disciplinary purposes where applicable.

When monitoring emails, the trust will, save in exceptional circumstances; confine itself to looking at the address and heading of the emails. Workers should mark any personal emails (where these are permitted by the trust) as such and encourage those who send them to do the same. The trust will avoid, where possible, opening emails clearly marked as private or personal.

The trust considers the following to be valid reasons for checking an employee's email:

- if the employee is absent for any reason and communications must be checked for the smooth running of the trust to continue;
- if the trust suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the trust understands that it is possible for workers inadvertently to receive such material and they will have the opportunity to explain if this is the case);
- if the trust suspects that an employee has been using the email system to send and receive an excessive number of personal communications (or any personal emails if this is prohibited by the trust); and
- if the trust suspects that the employee is sending or receiving emails that are detrimental to the trust or its pupils.

The trust may monitor communications without notification in certain specific circumstances, including but not limited to;

- establish the existence of facts relevant to the trust e.g. whether a contract was entered into by email;
- ascertain compliance with regulatory or self-regulatory practices e.g. checking that the trust is complying with external or internal regulations;
- ascertain or demonstrate standards that are or ought to be achieved by workers using the system;
- investigate or detect unauthorised use of the telecommunication system, which would include checking

that workers are not breaching the trust's policy on email and internet use; and
- ensure the effective operation of the system, for example through virus monitoring.

Monitoring will be reasonable and in accordance with current legislation. CEO/EHT approval will be required.

10. Covert monitoring

The use of covert monitoring will only be used in exceptional circumstances, for example, where the trust suspects criminal activity or where telling the employee about the monitoring would make it difficult to prevent or detect such wrongdoing.

If the trust considers covert monitoring to be justified, this will only take place as part of a specific investigation, and will cease when the investigation has been completed. CEO/EHT approval will be required. Misuse of the facility to monitor an employee's email account will be a conduct issue and dealt with via the discipline policy.

11. Routine or random monitoring of equipment

Some workers have the exclusive use of mobile or fixed technology. To ensure the acceptable use of ICT agreement is being adhered to by all workers, the CEO/Executive Headteachers may from time to time examine individual devices. This will be by arrangement and devices will be selected at random.

12. Trust expectations for the use of TEAMS

1) All behaviour should be professional.
2) The background must be blurred, where there is a technical problem the background must be blank.
3) If there are difficulties finding a room where you can be alone please let the meeting lead know. Staff can use school / Trust offices if needed.
4) Attention should be paid as to those sharing your space at home or at work. Where other people are likely to be in the room please alert meeting members before the meeting. In this case confidential information should not be discussed.
5) Unless previously agreed for the meeting to be a 'working lunch', no food should be consumed.
6) Dress should be as per the Code of Conduct.
7) General body language and behaviour should be professional and in accordance to Trust expectations.
8) Email should be used to send confidential information and TEAMS chat should not be used for this transferal.
9) No smoking throughout.
10) The screen used should reflect work and purpose, if using a second screen this should be out of view.

12. Trust expectations for remote working

- Staff will only use the Trust's email/internet/learning platforms and any related technologies for professional purposes or for use deemed appropriate and 'reasonable' by the Head of School, Executive Headteacher or Trustees.
- Staff will comply with the IT system security and not disclose any password provided to me by the Trust, School or other related authorities.
- Staff will ensure that all electronic communications with stakeholders are strictly professional.
- Staff will not give out my personal details, such as my mobile phone number, personal e-mail address and/or social networking identities to other stakeholders (parents/carers or pupils).
- Staff will ensure that personal data (such as data held on MIS software (i.e. Scholar Pack) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head of School or Executive Headteacher. Personal or sensitive data taken off site must be encrypted.
- Staff will not install any hardware, on any school machines, without the permission of the Head of School. This includes the usage of school hardware that is loaned out to pupils/families.
- Staff will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. This includes school hardware that is loaned out to pupils/families.

- Images and/or recordings (including voice recordings) of stakeholders will only be taken, stored and/or used for professional purposes in line with the Trust policy and with written consent of the parent, carer or staff member. Images will never be distributed outside the school network without the permission of the parent/carer, member of staff or Head of School.
- Staff will understand that all use of the Internet and digital learning platforms (and any other related technologies) can and will be monitored and logged. Data and information logged from these actions can be made available upon request and will be facilitated by the Head of School.
- Staff will respect copyright and intellectual property rights.
- Staff will ensure that online activity, both in school and outside school, will at all times remain professional and in accordance with school policy and it will not bring The Trust into disrepute.
- No stakeholder (child or parent/carer) will ever be online 1-1 with a member of school staff, at any point.
- Staff will support, promote and uphold the values set out in the Trust's online safety and data security policies and will help all stakeholders to be safe and responsible in their use of ICT and related technologies.

Appendix E – Dress Code

The way we present ourselves gives an important first impression, not only of ourselves but of the whole school. We believe our pupils have the right to be in an environment that makes them feel safe, does not make them feel uncomfortable and gives them high aspirations. No adult will be discriminated against in the area of dress and appearance on the grounds of gender, race, religion, disability or background. This code has been formulated in line with the school's overall 'Equality Statement'. Staff should wear clothing that:

- is appropriate to their role;
- is not likely to be viewed as offensive, revealing, or sexually provocative;
- does not distract, cause embarrassment or give rise to misunderstanding;
- is absent of slogans;
- is not considered to be discriminatory and is culturally sensitive;
- does not place themselves or others at risk.

Suitable clothing

- Smart trousers
- Dresses
- Skirts
- Shirt and tie or smart blouse/top

Footwear must be safe, sensible, in good order, smart and clean and have regard to medical or health and safety considerations. Employees need to be aware that in an emergency situation, they may be required to move swiftly. Therefore, by wearing high heeled, open-toed or open-backed types of footwear, they may put themselves at risk of injury. In such an event, the school will take no responsibility for any injuries thus incurred.

Headgear worn for religious purposes is permitted. It must be adjusted in a way that the wearers face remains visible and should be fixed in such a way that it allows quick release.

Extra-curricular

If there is a need to wear sports clothing for PE, please change back into work wear straight after the session.

When taking part in school visits, staff should wear comfortable clothing that is suitable for the activity taking place, considering all of the above.

Hair, tattoos and piercings

Hair should not be brightly coloured or styled dramatically and any tattoos should be covered, in line with HEARTS values. Unusual piercings must be kept hidden or removed.

Housekeeping staff

Housekeeping staff should wear clothes which are appropriate for their work and do not cause any health and safety concerns. Hair should be tied back, and appropriate PPE worn where provided.

If you are unsure what to wear for work please ask the Head of School or senior member of staff who will be able to advise you.

Additional clarity regarding the dress code:

- For clarity, leggings may not be worn as they are not a 'smart trousers'.
- 'Ugg' boots or 'style of' are not part of the dress code.
- Staff polo shirts may be worn for PE, school trips or for days when not working directly with children.
- In the line: Shirt and tie or smart blouse/top, 'top' is defined as a tunic. A smart jumper or cardigan may be worn over the 'shirt and tie or smart blouse/top'.

Head of Schools may adjust the dress code in line with weather conditions for brief periods if they feel it is appropriate.