Code of Conduct for employees

Ivy Learning Trust's Code of Conduct for employees is agreed by the Trust Board. It will be reviewed annually.

Date agreed: 16 July 2024 **Agreed by:** Trust Board **Review date:** September 2025

Last review date: 11 July 2023

Inclusion

The Ivy Learning Trust carefully considers all policies with respect to the impact on equality and the possible implications for pupils and staff with protected characteristics.

As part of the process of drafting this policy, consideration has been given to any potential impact on those with protected characteristics within Ivy:

Protected characteristic	**Impact**	**Protected characteristic**	**Impact**
Age	Neutral	Pregnancy/ maternity	Neutral
Sex	Neutral	Marriage/ civil partnership	Neutral
Disability	Neutral	Gender reassignment	Neutral
Ethnicity, race and culture	Neutral	Religion or belief	Neutral
Sexual orientation	Neutral		

Introduction

The expectations are that all pupils receive the highest possible quality of teaching and learning within a positive and respectful environment. It is important, therefore, that employees and workers understand that their own behaviour and the manner in which they conduct themselves sets an example and affects the school environment.

The Trust recognises that the majority of employees and workers always act in an appropriate, professional manner and treat others with dignity and respect. However, we consider it important to make clear the standards we expect so that breaches, misunderstandings and/ or misinterpretation of rules are kept to a minimum.

The Code is binding on all Ivy Learning Trust employees. It is also expected that other workers deployed within the trust will adhere to its principles. Similarly, volunteers are also expected to adhere to the principles set out in the Code and should consider themselves to fall into the category of 'worker' whilst within the Ivy Learning Trust for that purpose. Trustees are expected to follow the separate 'Code of Conduct for Trustees'. Members of Local Governing Boards are expected to follow the separate 'Code of Conduct for Members of LGBs'.

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 act in the best interests of the school and its pupils.

It should be noted that it is the normal practice of this Trust to require all employees and workers to sign, on a regular basis, a declaration to confirm that their criminal record is unchanged, that there are no investigations or charges pending and, in relevant circumstances, that they are not disqualified from working in certain roles and/or provision under the Childcare Act 2006. The declaration also includes a requirement to confirm acceptance of this Code of Conduct and the rules contained within it.

If there is anything in this Code that you do not understand, you should speak to your Line Manager or the Head teacher.

Failure to adhere to the Code of Conduct for employees may result in disciplinary action taken against you in accordance with the Disciplinary Policy.

Vision and values to be followed by all staff

Ivy's vision: Ivy is a charity whose purpose is to provide education for the public benefit

Ivy's values:

- We are one family of schools
- A good education is a birthright
- We want to make it easy to make a difference
- We believe local leaders know their schools best

School values: each school has its own set of values

General requirements and expectations

The school has high standards and expectations of all employees and workers. Therefore, it is required that you:

- provide a high standard of service in your dealings with members, trustees, governors, colleagues, pupils, parents/ carers, and other stakeholders whether this is in person, by telephone, letter or email. Always be polite, responsive and treat people with respect and consideration. Be as clear as possible about any decisions and actions you take and the reasons for them;
- act in a professional manner at all times;
- always use appropriate language and never demean, distress or offend the decency of others. This may happen, for example, by displaying material or pictures that could be seen as offensive, or by making degrading, suggestive or insensitive comments or remarks;
- do not make derogatory comments or seek to undermine members, trustees, governors, senior leaders or other employees/ workers;
- respect the rights of others and treat them with dignity;
- never threaten, bully, fight with or assault anyone;
- never steal, damage or take items that belong to others and that you hand any lost property in to the school office;
- do not discriminate against, harass or victimise anyone you meet in the course of your work, on any grounds;

- raise any concerns about inappropriate behaviour by pupils, parents/ carers or colleagues, or about the internal workings of the school or the Ivy Learning Trust, by following the appropriate procedure. (Members of a Professional Association/ Trade Union should also observe any Code, or rules, it has in place in relation to dealings with colleagues);
- positively promote the school's vision, ethos and values;
- comply with school policies and any other rules, regulations or codes that apply to your work and the workplace;
- use electronic media communications appropriately, responsibly and legally at all times, whether within or outside the workplace/ working hours;
- do not make public statements about the school without first obtaining authorisation from the Head;
- avoid actions that may discredit the school or bring it into disrepute;
- ensure that you are not under the influence of alcohol during working hours (the Head will decide if it is appropriate for alcohol to be made available at staff parties/ social events) and do not abuse drugs;
- do not disclose or misuse confidential information;
- do not engage in, or encourage, gossip, rumour or innuendo.

Safeguarding

Ivy Learning Trust is committed to safeguarding and promoting the welfare of children and young people. Therefore, as an employee within the Trust, you have a duty to safeguard pupils from harm (including physical, emotional and sexual abuse, or neglect), and to report any concerns you have.

- You must read the the most up to date DfE statutory guidance on 'Keeping Children Safe in Education'; and act in accordance with the principles and procedures set out within it at all times;
- You must ensure that you read and understand Ivy's Safeguarding and Child Protection policy and that you are aware of the processes to follow if you have concerns about a child;
- Reading and confirming compliance with the Safeguarding and Child Protection policy will from part of the induction process for new staff;
- Our safeguarding policy and procedures are available on the Trust Policies drive, in the staff room and from the school office.

Low Level Concerns

- The definition of low level concerns can be found on the Ivy Safeguarding and Child Protection Policy. Please refer to this if you require guidance. The procedures are clearly outlined in the policy.

Staff/ pupil relationships

All staff will observe proper boundaries with pupils that are appropriate to their professional position. You must ensure that you do not breach professional boundaries and do not act in a way that could be misinterpreted or otherwise leave you vulnerable to allegations of inappropriate behaviour. You should avoid contact with pupils outside of school hours if possible.

In particular, in relation to contact with pupils, you must:

- not establish, or seek to establish, social contact with pupils (inc. former pupils under the age of 18) or aim to secure a friendship or strengthen a relationship, for any reason. You must exercise your professional judgement in making an appropriate response if a pupil seeks to establish social contact with you or if contact should occur accidentally;

- not buy or give gifts to children (inc. former pupils under the age of 18) other than as part of a school rewards system;
- not give to, or exchange with pupils (inc. former pupils under the age of 18), any personal details such as home/ mobile phone number or home or personal e-mail address for any reason, nor must you exchange any private texts, information or photos of a personal nature, unless a specific need to do so is agreed with your Line Manager or the Head;
- not offer or give lifts to pupils (inc. former pupils under the age of 18) in your personal vehicle.

If staff members and pupils must spend time on a one-to-one basis, staff will ensure that:

- this takes place in a public place that others can access
- others can see in to the room
- a colleague or line manager knows this is taking place.

If a staff member is concerned at any point that an interaction between themselves and a pupil may be misinterpreted, this should be reported to their line manager or the Head.

Income generation

Anyone filming or taking photographs on school or Ivy Learning Trust premises to generate income for personal use must agree to the following:

- No child should appear in photographs or videos. In exceptional circumstances prior consent may be obtained from the child's parent / carer, subject to permission from the Senior Leadership Team.
- The school / Trust can only be named on campaigns agreed and approved by the Senior Leadership Team or Ivy Learning Trust Central Team.
- Time spent making videos must not in any way impact on the education of the children (this will be judged by the Senior Leadership Team).
- Any additional income generating activities must be done out of school hours and not cause a conflict of interest to the staff member's permanent job (see section on secondary employment).
- Staff will not use personal mobile phones and laptops, or school equipment for personal use, in school hours or in front of pupils. They will not use personal mobile phones or cameras to take pictures of pupils.
- All videos filmed at an Ivy Learning Trust school or site must be approved by a member of the school's Senior Leadership Team or Ivy Central Team before being posted on social media.

Communication and social media

The Trust recognises the benefits and opportunities which a social media presence offers. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and reputation. This policy aims to encourage the safe use of social media by schools, staff, parents / carers and children.

Staff may not engage in inappropriate use of social media sites which may bring themselves, the school, the Trust into disrepute. Staff should not upload any content on to social media sites that:

- is confidential to the school / Trust or its staff
- amounts to bullying
- amounts to unlawful discrimination, harassment or victimisation
- brings the school / Trust into disrepute

- contains inappropriate or offensive content
- undermines the reputation of the school and / or individuals
- is defamatory or knowingly false
- breaches copyright
- is in any other way unlawful

Staff should exercise caution in their use of social media sites or any web based presence they have, including written content, videos or photographs, and views expressed either directly or indirectly, for example, by 'liking' certain pages or posts established by others.

School staff's social media profiles should not be available to pupils. If they have a personal profile on social media sites, they should not use their full name, as pupils may be able to find them. Staff should consider using a first and middle name instead, and set public profiles to private.

Staff should not attempt to contact pupils or their parents/ carers via social media, or any other means outside school, in order to develop any sort of relationship. They will not make any efforts to find pupils' or parents/ carers' social media profiles.

Staff will ensure that they do not post any images online that identify children who are pupils at the school without consent from the child's parent / carer.

Acceptable use of technology

Staff will not use technology in school to view material that is illegal, inappropriate or likely to be deemed offensive. This includes, but is not limited to, sending obscene emails, gambling and viewing pornography or other inappropriate content.

Staff will not use personal mobile phones and laptops, or school equipment for personal use, in school hours or in front of pupils. They will not use personal mobile phones or cameras to take pictures of pupils.

We have the right to monitor emails and internet use on the school IT system. Please see appendix A for more information.

Conduct outside of work

Staff will not act in a way that would bring the school, or the teaching profession, into disrepute. This covers relevant criminal offences, such as violence or sexual misconduct, as well as negative comments about the school on social media.

Secondary employment

The Working Time Regulations 1998, as amended, are a Health and Safety initiative and cover all work undertaken. To enable Ivy to comply with the Regulations and maintain the health and safety of all employees, you must inform your Line Manager of ALL work undertaken, or applied for, elsewhere (should you be engaged in, or intending to be engaged in, other paid or unpaid work).

In addition, it is important you are aware that there should be no conflict of interest, nor any contractual conflict, between your work for the Trust and your work elsewhere. Approval to undertake, or continue with, secondary

employment can only be granted in circumstances where there is no conflict with the provisions of the Working Time Regulations nor any other conflict of interest or contractual conflict.

Note in particular that support staff on Scale 6 and below will not unreasonably be refused permission to undertake secondary employment unless there is a clear conflict of interest, contractual conflict or a potential breach of the Working Time Regulations.

Any employee asked to undertake private tutoring of pupils within the school must first discuss the situation with the Head.

General working standards

- It is important that all employees and workers are in the workplace at their agreed starting time and do not leave before their agreed finishing time
- You must therefore attend work in accordance with your contract of employment and associated terms and conditions in relation to hours, days of work and holidays
- Wherever possible, you should make routine medical and dental appointments outside of your working hours or during holidays. The only exceptions to this requirement will normally be in the event of an emergency, particular difficulty in relation to hospital appointments (which are rarely negotiable) or to attend for ante-natal care if you are pregnant. Pregnant employees are entitled to paid time off for ante-natal appointments. In any circumstances, however, you should agree time off with your manager at the earliest opportunity to ensure that adequate cover arrangements can be made
- Prior to making any request, you should refer to your school's policy on special leave if you need time off for any reason other than personal illness. It is important to note that, except in cases of serious urgency, no employee may without prior permission, be absent from duty for any cause other than personal illness.

Sickness absence reporting

All staff are expected to follow the school's Absence Reporting Procedure when they are absent from work due to illness or injury. This procedure includes notification as early as possible on the first day of absence, keeping the school informed where absence continues, requirements for the provision of 'Statements of Fitness for Work' and procedures on return to work.

Appearance and dress

It is expected that:

- when at work, or representing the school, you ensure that your appearance is neat and clean
- you always dress in a manner which is appropriate to your role and the circumstances or setting in which you work
- you remember that you are a role model for pupils and your appearance and dress should reflect this important and unique position
- you do not dress in a way that may cause embarrassment to pupils, parents/ carers, colleagues, governors, other stakeholders or visitors.

Ultimately, it will be for the Head to decide whether an employee's/ worker's appearance and/ or dress is appropriate or not. They must ensure that the rights of employees to dress as they please, and in accordance with their principles and beliefs, is balanced with the need for the school to promote a suitable image to its stakeholders. At all times, care will be taken not to discriminate in relation to appearance and dress requirements.

Confidentiality

In the course of their role, members of staff are often privy to sensitive and confidential information about the school, staff, pupils and their parents/ carers. This information will never be:

- Disclosed to anyone without the relevant authority;
- Used to humiliate, embarrass or blackmail others;
- Used for a purpose other than what it was collected and intended for.

Staff members must abide by the General Data Protection Regulations 2018 (see Data Protection policy). This does not overrule staff's duty to report child protection concerns to the appropriate channel where staff believe a child is at risk of harm.

Honesty and integrity

Staff should maintain high standards of honesty and integrity in their role, in accordance with The Seven Principles of Public Life. This includes when dealing with pupils, handling money, claiming expenses and using school property and facilities.

Staff will not accept bribes. Gifts that are worth more than £50 must be declared and recorded on the gifts and hospitality register.

Staff will ensure that all information given to the school about their qualifications and professional experience is correct.

There may be occasions when there is scope for conflict between an employee or worker's own interests and those of the school. It is important that such interests are clearly documented. Therefore, to avoid any difficulties arising from a potential clash of interests you must:

- notify your Manager or the Head if you have links, of any sort, with an outside organisation which may carry out work for the school, or supply it with goods or services (or is tendering or preparing to do so);
- not participate in any staff recruitment process, where you are related to, or have a close personal relationship with an applicant;
- not participate as part of any recruitment process or other panel if you may be in a position to benefit from the outcome;
- avoid acting as a professional representative on behalf of a friend, partner or relative in any business or commercial dealings they have with the school;
- report any possible conflict of interest to your manager or the Head teacher;
- all staff Members of LGBs must provide the information requested on the Declaration of Interests form for inclusion in the Register of Business Interests published on the Ivy website .

Links with other policies and procedures

All employees and workers, as appropriate, must comply with the Trust's policies (available in the Trust Google Drive) and individual school procedures.

In addition, teachers are expected to uphold and adhere to the standards of 'Personal and Professional Conduct' as set out in part Two of the Teachers' Standards as published by the Department for Education.

APPENDIX A

Acceptable Use Agreement

Introduction

This agreement is designed to enable acceptable use for staff and governors.

The School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of both staff, governors and pupils, it is important that all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure.
- Define and identify unacceptable use of the school's ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and school devices.
- Specify the consequences of non-compliance.

This policy applies to staff members and governors, and all users of the School's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to the IT Network and Data Manager or the school's responsible IT person (Please speak to the headteacher to confirm who this is).

Provision of ICT Systems

All equipment that constitutes the School's ICT systems is the sole property of the School.

No personal equipment should be connected to or used with the School's ICT systems. Users must not try to install any software on the ICT systems without permission from the IT Network and Data Manager or the school's responsible IT person. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

The IT Network and Data Manager is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Users are not permitted to make any physical alteration, either internally or externally, to the School's computer and network hardware.

Network access and security

All users of the ICT systems at the School must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed as enforced by the Schools security policies and must consist of 8 characters with a mixture of letters, numbers and symbols.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them with any other person, except to designated members of the school and Trust IT team for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the IT Network and Data Manager or headteacher as soon as possible.

Users should only access areas of the schools computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the school ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the school ICT systems or cause difficulties for any other users.

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.

School Email

Where email is provided, it is for academic and professional use, with no personal use being permitted. The School's email system can be accessed from both the school computers, and via the internet from any computer. Wherever possible, all school related communication must be via the school email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email or password protection.
- Emails should never contain children's full names either in the subject line and preferably not in the main body of the text. Initials should be used wherever possible.
- Access to school /setting email systems will always take place in accordance with data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts unless permitted by the head teacher or ITNDM.

- Email passwords must be regularly changed as enforced by the Schools security policies and must consist of 8 characters with a mixture of letters, numbers and symbols.
- Emails must only be kept for as long as operationally necessary and in line with the trust's retention policy (2 years).

Internet Access

Internet access is provided for academic and professional use, with no personal use being permitted.

The School's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to the IT Network and Data Manager or the schools responsible IT person.

Staff must not therefore access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the School and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary such information may be handed to the police in connection with a criminal investigation.

Digital cameras

The school encourages the use of digital cameras and video equipment; however staff should be aware of the following guidelines:

- Photos should only be named with the pupil's name if they are to be accessible in school only. Photos for the website or press must only include the child's first name.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones.

- All photos should be downloaded to the school network
- The use of mobile phones for taking photos of pupils is not permitted.

File Storage

Staff members have their own personal area on the network and Google Drive, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

- If information/data has to be transferred it must be saved on an encrypted, password protected, storage device
- No school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

External Storage Devices

External storage devices, such as the following:

- USB Drives
- USB Hard drives
- CD's
- DVD's
- Personal cloud based storage

Are not permitted under any circumstances without permission of the Head Teacher or IT Network and Data Manager, as a result the above devices will not be provided or supported.

Mobile Phones

Mobile phones are permitted in school, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker.
- Personal mobile phone cameras are not to be used on school trips. The school may provide the relevant equipment for this purpose.
- All phone contact with parents regarding school issues will be through the schools phones. Personal mobile numbers should not be given to parents at the school.

Monitoring of the ICT Systems

The school may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the school's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. The network is regularly checked by the IT Network and Data Manager or the school's responsible IT person to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other school policy;

- investigate a suspected breach of the law, this policy, or any other school policy.

Door Access Control

Fobs/passes and codes are issued to staff as needed and should not be shared with anyone unless authorised to do so by the IT Network and Data Manager or headteacher. Where fobs are issued these should be kept secure and the holder must know where it is at all times, should a fob become lost or misplaced the IT team must be notified immediately to prevent unauthorised access. The school and trust may hold the individual personally liable for any lost or misplaced fob and impose a charge of £5 to cover a replacement.

Failure to Comply with the Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Any unauthorised use of the school's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the IT Network and Data Manager or the schools responsible IT person considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The school reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Acceptable Use Agreement

To be completed by all staff, governors and student/agency teachers

As a school user of the network resources/ equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the school rules (set out within this policy) on its use. I will use the network/ equipment in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the IT Network and Data Manager or the school's responsible IT person.

I agree to report any misuse of the network to the IT Network and Data Manager or the school's responsible IT person. Moreover, I agree to report any websites that are available on the school internet that contain inappropriate material to the IT Network and Data Manager or the school's responsible IT person. I finally agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the IT Network and Data Manager or the school's responsible IT person.

Specifically when using school devices: -

- I must not use these devices for inappropriate purposes or personal use.
- I must only access those services I have been given permission to use.
- I will not download, use or upload any material which is unsuitable within a School setting or that may cause disruption to the School network.
- I must not use any external storage devices.
- I am aware that should I lose or misplace my fob/pass I may be charged a replacement fee of £5.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the School will monitor communications in order to uphold this policy and to maintain the School's network (as set out within this policy).

Signed …….. Date ……..

Print name ……