ONLINE SAFETY

Date of Next Review: September 2025

Responsible Officer: CEO

Table of Contents

Statement of Intent

Vision 1590 Trust understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout Trust schools; therefore, there are several controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. This policy has been created with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils, staff and visitors.

1. Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Child Protection, Safeguarding & Child on Child Abuse Policies
- Anti-Bullying Policy
- RSHE Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Pupil Remote Learning Policy

2. Roles & Responsibilities

The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date by undertaking training.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.

- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- Communicate regularly with parents to reinforce the importance of children being safe online.
- as part of the shortlisting process, consider carrying out an online search as part of their due diligence on shortlisted candidates to help identify any incidents or issues that have happened, and are publicly available online which the school/ academy might want to explore with applicants at interview.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.

- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an annual basis.

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted regularly on the topic of remaining safe online

Handling Online Safety Concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the victim.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher will contact the police.

The school will avoid unnecessarily criminalising pupils. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

4. Cyber Bullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating, discriminatory or upsetting messages
- Threatening or embarrassing media sent via electronic means
- Silent or abusive phone calls or using the victim's device to harass others, to make them think the victim is responsible
- Unpleasant or defamatory information/comments/messages posted online
- Abuse between young people in intimate relationships online

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

5. Child-on child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Voyeurism and Upskirting

- Sexualised online bullying
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy.

The school responds to all concerns regarding online child-on-child sexual abuse and harassment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with their child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including but not limited to:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay.

7. Mental Health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media platforms and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

8. Online Hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the

distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

9. Cyber Crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

In addition, the school will implement a cyber awareness plan for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cyber crime.

The school will implement it's cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges' and the Cyber Security Policy.

10. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11. Online safety and the curriculum

The school references the DfE 'teaching online safety in schools' guidance during the creation of their curriculum. Online safety is embedded throughout the curriculum and teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. For more information on the risks considered consult the DfE's 'teaching online safety in schools' guidance.

The DSL is involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

12. Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Laptop/Desktop Computers
- Mobile/Tablet Devices
- Internet and Email
- Photo/Video/Audio equipment

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always review and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using technology and/or online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of technology.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom without explicit permission and appropriate technological safeguards in place.

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating Parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised by the school via methods such as

- Letters and newsletters
- School website and links to external online resources, e.g. Child Exploitation and Online Protection Command (CEOP)
- High profile events, such as Safer Internet Day
- Online Reporting

15. Internet Access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and agreed to the Acceptable Use Agreement.

All members of the school community are encouraged to use the school's network, instead of mobile networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately for their age group.

16. Filtering and monitoring online activity

The Trust use context appropriate differentiated filtering, based on age, vulnerability and risk of harm. All users are allocated to an appropriate role or age related/risk level group to facilitate variations in filtering strength. For example, an SEN student may be placed into a lower age bracket group to safeguard them more appropriately.

The filtering technology used is:

- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

The Trust have overall strategic responsibility for filtering and monitoring. The Trust and Head teachers identify members of the leadership team in each school to be responsible to ensure effective implementation and management.

School leaders will work closely with the designated safeguarding lead (DSL) and IT support providers in all aspects of filtering and monitoring. Day to day management of the filtering and monitoring system will be conducted by the DSL and IT support provider.

Periodic Reviews and Monitoring

The Trust will review the filtering and monitoring solution:

- at least annually
- when a risk is identified
- following changes to school curriculum
- in response to changes in working practice
- when new technology is introduced

IT Providers will conduct periodic reviews to ensure:

- That the system has not been changed or deactivated
- That setting appropriate filtering and reporting remains active
- Ensure training and advice requirements are met
- Record the details of all checks and reviews conducted as well as any resulting actions identified

DSL and Safeguarding staff will:

- Respond promptly and proportionately to concerns raised by automated alerts and disclosures made
- Liaise with the IT support provider to ensure setting appropriate filtering and reporting remains active
- Address changes to curriculum and local safeguarding concerns
- Review blocklist and modify in line with changes to safeguarding risks

- Review blocklists to ensure the filtering and monitor systems employed do not negatively impact upon teaching and learning
- Ensure all staff, students and visitors know how to report and record concerns
- Provide training to staff, students and visitors

The Impact on Teaching and Learning

The filtering and monitoring solutions employed must block internet access to harmful sites and inappropriate content. However, it will not:

- unreasonably impact teaching and learning or school administration
- restrict students from learning how to assess and manage risk themselves

The filtering and monitoring solution applies to all users including guest accounts, school owned devices and any other device using the school broadband and will:

- filter all internet feeds, including any backup connections
- be age and ability appropriate for the users, and be suitable for educational settings
- handle multilingual web content, images, common misspellings and abbreviations
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- log activity by date and time along with the device name or ID, IP address and where possible the individual
- provide alerts when any web content has been blocked in accordance with the local setting requirements

Deliberate breaches of the filtering system are reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Child Protection and Safeguarding Policy.

17. Network Security

A layered approach to security is taken at the school and is managed by ICT technicians. Antivirus security software is installed and kept up to date. Device firewalls are switched on at all times and application controls are employed to restrict access.

Staff and pupils are not to permitted to download/run unapproved software and must remain vigilant to threats from malicious email attachments. Staff and students are expected to report any incidents to the ICT technicians.

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils are provided with either their own unique username and private passwords or a shared account as appropriate. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their private login details with others and are not allowed to log in as another user at any time.

Users are required to lock access to devices and systems when they are not in use.

18. Emails

Staff and pupils are given approved school email accounts. Prior to being authorised to use the email system, staff and pupils must agree to the Acceptable Use Agreement. Personal email accounts are not permitted to be used for school. Any email that contains sensitive or personal information is only sent securely via encrypted email.

Staff are not permitted to communicate with pupils or parents via personal email accounts.

Staff members and pupils are required report junk/phishing messages. The school's email system can is configured to reduce threats from emails and attachment.

Multi-Factor Authentication is enforced for all staff accounts and staff receive regular cyber security-awareness training.

Any cyber-incidents are managed in line with the Data and Cyber-security Breach Prevention and Management Plan.

19. Generative Artificial Intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

20. Social Networking

Personal use

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff are not permitted to communicate with pupils or parents over social networking sites in an official capacity and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy.

Use on behalf of the school

The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

21. The school website

The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website.

22. Use of Devices

School-owned devices

Staff members may be issued with devices such as laptops, tablets, mobile phones or cameras to assist with their work.

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum.

School-owned devices are used in accordance with the acceptable use agreements. Mobile school-owned devices are managed via a Mobile Device Management (MDM) Solution and are both encrypted and password protected.

ICT technicians monitor school-owned devices and automate the installation of software updates and antivirus definitions. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behavioural Policy respectively.

Personal devices

Any personal electronic device that is brought into school is the responsibility of the owner/user.

Students are not permitted to use personal devices on site during school hours without explicit permission of the school.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils. Staff members are not permitted to store student/staff personal data on personal devices.

Staff members must report concerns about their colleagues' use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy.

Where a pupil uses accessibility features on a personal device to help them access education, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

23. Remote learning

All remote learning is delivered in line with the school's Pupil Remote Learning Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with

parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

During the period of remote learning, the school will maintain regular contact with parents.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software on devices not owned by the school.

24. Monitoring and Review

The governing board, headteacher and DSL review this policy in full on an **annual** basis and following any online safety incidents.

The next scheduled review date for this policy is **September 2025**.

Any changes made to this policy are communicated to all members of the school community.

Online harms and risks – curriculum coverage

[The table below contains information from the DfE's 'Teaching online safety in schools' guidance about what areas of online risk schools should teach pupils about. You can use this to assist your school in developing its own online safety curriculum; however, you must develop your curriculum in line with your local needs and the needs of your pupils.]

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm will be covered in the following curriculum areas: • Health education • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching will include the following: • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE • Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships and health education • [Secondary schools] RSHE • [KS2 and above] Computing

	• That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	• [KS3 and KS4] Citizenship
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching will include the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE • Computing
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following: • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim • How to protect yourself and others against different types of online fraud • How to identify 'money mule' schemes and recruiters • The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details • How to report fraud, phishing attempts, suspicious websites and adverts	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE • Computing
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following:	This risk or harm will be covered in the

	• Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE • Computing
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE • Computing
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following: • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue • How notifications are used to pull users back online	This risk or harm will be covered in the following curriculum areas: • Health education • Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following: • How to find information about privacy settings on various sites, apps, devices and platforms • That privacy settings have limitations	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE • Computing
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching will include the following:	This risk or harm will be covered in the

	• How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE • Computing
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE • Computing • [KS4] Citizenship
Radicalisation	Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following: • How to recognise extremist behaviour and content online • Which actions could be identified as criminal activity • Techniques used for persuasion • How to access support from trusted individuals and organisations	All areas of the curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE

	• How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE
Fake profiles	Not everyone online is who they say they are. Teaching will include the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE • Computing
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE
Livestreaming	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching will include the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content	This risk or harm will be covered in the following curriculum areas: • [Secondary schools] RSHE

	• That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That pupils should not feel pressured to do something online that they would not do offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming	
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching will include the following: • That pornography is not an accurate portrayal of adult sexual relationships • That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour • That not all people featured in pornographic material are doing so willingly, e.g. revenge porn or people trafficked into sex work	This risk or harm will be covered in the following curriculum areas: • [Secondary schools] RSHE
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE • Computing
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching will include the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • That 'easy money' lifestyles and offers may be too good to be true • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm will be covered in the following curriculum areas: • [Secondary schools] RSHE

Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching will include the following: • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	This risk or harm will be covered in the following curriculum areas: • Health education
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching will include the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm will be covered in the following curriculum areas: • [Primary schools] Relationships education • [Secondary schools] RSHE
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching will include the following: • Strategies for positive use • How to build a professional online profile	This risk or harm will be covered in the following curriculum areas: • [Secondary schools] RSHE
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	

Appendix 2 – Technology acceptable use agreement for pupils

Vision 1590 Trust understands the benefits technology can have on enhancing the curriculum and pupils' learning; however, we must ensure that pupils respect school property and use technology appropriately. To achieve this, we have created this acceptable use agreement which outlines our expectations of pupils when using technology, whether this is on personal or school devices and on or off the school premises.

Please read this document carefully and sign below to accept that you agree to the terms outlined.

User Accounts

- Pupil accounts are to be used by the assigned user / group for academy related and educational purposes, personal professional development and careers purposes only.
- Accessing or attempting to access another user's account is strictly prohibited.
- Pupils are required to take all necessary precautions to keep their account secure and must not share their personal account or password with others.

Use of Technology

- Pupils will only use Trust systems and devices that they have been given permission to access.
- Pupils must adhere to the online safety guidelines they have been taught.
- Pupils must not store or use personal data relating to a pupil or staff member for non-school related activities on Trust systems and devices.
- At school, during school hours pupils must only use the internet for school related activities.
- Pupils must not attempt to download and run or install additional software on school owned devices.
- Pupils must delete emails from unknown senders without opening them and must not open any email attachments or links they contain.
- Pupils must behave responsibly and not interfere with teaching and learning whilst using Trust systems and devices.
- Trust systems and devices are subject to UK law. Pupils must not use the systems to upload, download, use, retain, distribute, create or access any electronic materials which:
    - May constitute a threat, bullying or harassment,
    - May be slanderous, abusive, indecent, obscene, racist, illegal or offensive.
    - May be a breach of copyright and/or licence provisions
    - Might gain access to restricted or unauthorised areas of the system and/or network, website or other hacking activities
- Pupils must not use the Trust systems for mass unsolicited mailings, commercial activity or the dissemination of junk mail, viruses or malware.
- Pupils must not attempt to "hack" or gain access to permissions, resources or systems that they are not permitted to access.

Personal Devices

- Direct connection to Trust networks of devices not supplied by the Trust is not permitted.
    - Pupils with permission to use a personal device, such as a laptop must connect to the guest Wi-Fi network at the school. Please speak to an ICT Technician for assistance.
- Personal mobile devices, such as mobile phones, tablets and media players must not be used on the school site and pupils must adhere to the school's mobile phone rules.
- Personal devices must not be used to record images/audio of other students or staff.

Social Media

- Pupils will not use Trust devices to access personal social networking platforms
- Pupils must not communicate or attempt to communicate with staff members over personal social networking platforms or email.
- Pupils must not accept or send 'friend' or 'follow' requests from or to any staff member over personal social networking platforms
- Pupils must not publish any comments or posts about the school on any social networking platforms or websites which may affect the school's reputation.
- Pupils must not post or upload any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website or platform.

Reporting Misuse

- Pupils will ensure that they report misuse or breaches of this agreement by pupils or staff members by means of the school's reporting procedure
- Violations will be dealt with in line with the relevant policy e.g. Behavioural Policy or Child Protection and Safeguarding Policy

Agreement

I understand that my use of Trust systems and devices including the internet will be monitored. I acknowledge that I have read and understood these terms and ensure that I will abide by each principle.

Name of pupil:	
Class:	
Signed:	
Date:	

Appendix 3– Technology acceptable use agreement for staff, governors, volunteers and guests

Vision 1590 Trust understands the benefits technology can have on enhancing the curriculum and pupils' learning; however, we must ensure that staff, governors, volunteers and guests use technology appropriately.

To achieve this, we have created this acceptable use agreement which outlines our expectations for staff when using technology, whether this is on personal or school devices and on or off the school premises.

Please read this document carefully and sign below to accept that you agree to the terms outlined below.

Definitions

- Staff – Used to refer to all staff, governors, volunteers and guests
- Technology – Used to refer to all technological devices and systems

User Accounts

- User accounts are to be used by the assigned user / group for academy related and educational purposes, personal professional development and careers purposes only.
- Accessing or attempting to access another user's account is strictly prohibited.
- Staff are required to take all necessary precautions to keep their account secure and must not share their account or password with others.

Use of Technology

- Staff will only use Trust systems and devices that they have been given permission to access.
- Staff will only use their assigned email accounts for official purposes.
- Staff will not use personal email accounts to send and receive personal data or information
- Staff will not share sensitive personal data with any other staff, pupils or third parties unless explicit consent has been received.
- Staff will ensure that any personal data is stored in line with the UK GDPR.
- Staff must delete emails from unknown senders without opening them and must not open any email attachments or links they contain.
- During school hours staff must only use the internet for school related activities.
- Staff must not attempt to download and run or install additional software on school owned devices.
- Staff will only store data on removable media or other technological devices that have been encrypted or suitably pseudonymised.
- Trust systems and devices are subject to UK law. Staff must not use the systems to upload, download, use, retain, distribute, create or access any electronic materials which:

    - May constitute a threat, bullying or harassment,
    - May be slanderous, abusive, indecent, obscene, racist, illegal or offensive.
    - May be a breach of copyright and/or licence provisions
    - Might gain access to restricted or unauthorised areas of the system and/or network, website or other hacking activities
- Staff must not use the Trust systems for mass unsolicited mailings, commercial activity or the dissemination of junk mail, viruses or malware.
- Staff must not attempt to gain access to permissions, resources or systems that they are not permitted to access.

Personal Devices

- Staff will ensure that personal mobile devices are either switched off or set to silent/discrete mode during school hours, and will only make or receive calls in locations appropriate to do so.
- Staff will not use personal mobile devices to take photographs or videos of pupils or staff
- Direct connection to Trust networks of devices not supplied by the Trust is not permitted.
    - Personal devices, such as a laptop must connect to the guest Wi-Fi network at the school. Please speak to an ICT Technician for assistance.
- Staff will ensure that any school data stored on personal mobile devices is encrypted and/or pseudonymised.
- By adding school accounts to a personal device, staff consent to Mobile Device Management, giving permission for the school to erase and wipe data off the device if it is reported lost or as part of exit procedures.

Web and Social Media

- Staff representing the school online on websites or via school social media accounts will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- Staff will not communicate with pupils or parents over personal social networking sites or email. Contact with pupils or parents will be done through authorised channels.
- Staff must not accept or send 'friend' or 'follow' requests from or to any pupils or parents over personal social networking platforms
- Staff will ensure that they apply appropriate privacy settings to any social networking sites.
- Staff must not publish any comments or posts about the school on any social networking platforms or websites which may affect the school's reputation.
- Staff must not post or upload any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website or platform.
- In line with the above, staff will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.

Training

- Staff will ensure they participate in any online safety training offered to me, and will remain up-to-date with current developments in social media and the internet as practical.
- Staff will ensure they employ methods of good practice and act as a role model for pupils when using technology.

Reporting Misuse

- Staff will ensure that they adhere to any responsibility they have for monitoring pupils use of technology.
- Staff will ensure that they report misuse or breaches of this agreement by pupils or staff members by means of the school's reporting procedure
- Staff understand that violations to this agreement will be dealt with in line with the relevant policy and that disciplinary action may be taken in accordance with the Disciplinary Policy and Procedures.

Agreement

I understand that my use of Trust systems and devices including the internet will be monitored. I acknowledge that I have read and understood these terms and ensure that I will abide by each principle.

Name	
Signed:	
Date:	