Excalibur Academies Trust

Online Safety Policy

St John's Marlborough

Date of approval	February 2021
Approved by	CEO
Review date	February 2024

Registered Office: Excalibur Academies Trust, Granham Hill, Marlborough SN8 4AX
Registered in England and Wales
Company number: 8146633

Contents

1. Aims

Excalibur Academies Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, governors, Board members and trustees.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Trust in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident (where appropriate).

2. Legislation and guidance

This policy is based on the Department for Education (DfE) statutory safeguarding guidance on keeping children safe in education and specifically focuses on:

- Teaching online safety in schools.
- Preventing and tackling bullying or cyber bullying.
- Advice for Principals and school staff.
- Relationships and sex education (where applicable).
- Searching, screening and confiscation.

It refers to the Department's guidance on protecting children from radicalisation and accounts for existing legislation. This includes but is not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

The policy reflects the Education Act 2011, which provides teachers with stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is "good reason" to do so.

We account for the national curriculum to ensure that our programs of study educate students on online safety, sex and relationships. This policy also complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1. Trust Board and Local Governing Body

The Trust Board has overall responsibility for all policies and will ensure that any amendments are made when legislation changes.

The Local Governing Body (LGB) of each school has an overall responsibility for monitoring and holding the Principal to account for its implementation. The LGB will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The nominated safeguarding governor is responsible for ensuring online safety is monitored.

All governors will:

- Ensure that they have read and understand this policy.
- Sign and adhere to the terms outlined in the acceptable use agreement (Appendix 2).

3.2. Principal and Senior Leaders

The Principal is responsible for ensuring that staff understand the policy, and that it is being implemented consistently throughout the school.

- The Principal and another members of the leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation.
- The Principal and senior leaders are responsible for ensuring that staff receive suitable training which enables them to carry out their online safety roles and disseminate knowledge.
- The Principal and senior leaders will ensure that there is a system in place to allow for monitoring and support of those in the school who carry out the internal online safety role.
- The Strategic Leadership Team (SLT) will receive and review regular monitoring reports from the person responsible for online safety within the school.

3.3. The Designated Safeguarding Lead (DSL)

Details of the school DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents.

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety contains a self-audit for staff on online safety training needs.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Principal and/or governing board.

This list is not intended to be exhaustive.

In some schools there will be an online safety co-ordinator who is not the DSL. In this case it is important that this person is line managed by the DSL and the role is clearly defined.

3.4. The Network Manager

It is acknowledged that in some schools the Network Manager is from the Trust central team or from an external organisation.

The Network Manager at St John's Marlborough is Ben Callaghan and he is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check annually and monitoring the school's ICT systems continually.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in accordance with the school behaviour policy.

This list is not intended to be exhaustive.

3.5. Staff and volunteers

All staff, agency workers, contractors and volunteers are responsible for:

- Understanding, following, and implementing this policy.
- Agreeing and adhering to the terms of the acceptable use agreement (Appendix 2).
- Ensuring that pupils follow the school's terms on acceptable use (Appendix 1).
- Working with the DSL to ensure that online safety incidents are logged and dealt withappropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with in accordance with the schoolbehaviour policy.

This list is not intended to be exhaustive.

3.6. Parents

Parents are expected to:

- Ensure that their child has read, understood, and agreed to the terms of acceptable use (Appendix 1).
- Notify a member of staff of any concerns or queries regarding this policy.

Further guidance on keeping children safe online can be obtained from the organisations outlined below.

- Childnet International (www.childnet.com)
- UK Safer Internet Centre (www.saferinternet.org.uk)
- Internet Matters (www.internetmatters.org)
- Digital Parenting (www.vodafone.co.uk/mobile/digital-parenting)
- Thinkuknow (www.thinkuknow.co.uk)
- NetAware (www.net-aware.org.uk)
- Parent Zone (www.parentzone.org.uk/)

3.7. Visitors and members of the community

Visitors and members of the community who use the school's ICT systems will be made awareof this policy and be expected to follow it (where applicable). If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

4. Educating pupils about online safety and relationships

All pupils educated about online safety and relationships in accordance with the National Curriculum.

Primary

In **Key Stage 1** pupils will be taught to:

- Use technology safely and respectfully.
- Keep personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the Internet or other online technologies.

In **Key Stage 2** pupils will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

Caring friendships

- The characteristics of friendships, including mutual respect, truthfulness, trustworthiness, loyalty, kindness, generosity, trust, sharing interests and experiences and support with problems and difficulties.
- That healthy friendships are positive and welcoming towards others, and do not make others feel lonely or excluded.
- How to recognise who to trust and who not to trust, how to judge when a friendship is making them feel unhappy or uncomfortable, managing conflict, how to manage these situations and how to seek help or advice from others, if needed.

Respectful relationships

- The importance of respecting others, even when they are very different from them (for example, physically, in character, personality or backgrounds), or make different choices or have different preferences or beliefs.
- Practical steps they can take in a range of different contexts to improve or support respectful relationships.
- The conventions of courtesy and manners.
- The importance of self-respect and how this links to their own happiness.

- That in school and in wider society they can expect to be treated with respect by others, and that in turn they should show due respect to others, including those in positions of authority.
- About different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help.
- What a stereotype is, and how stereotypes can be unfair, negative or destructive.
- The importance of permission-seeking and giving in relationships with friends, peers and adults.

Online relationships

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).

Being safe

- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- About the concept of privacy and the implications of it for both children and adults; including that it is not always right to keep secrets if they relate to being safe.
- That each person's body belongs to them, and the differences between appropriate and inappropriate or unsafe physical, and other, contact.
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
- How to recognise and report feelings of being unsafe or feeling bad about any adult.

- How to ask for advice or help for themselves or others, and to keep trying until they are heard.
- How to report concerns or abuse, and the vocabulary and confidence needed to do so.
- where to get advice e.g. family, school and/or other sources.

Mental Wellbeing

- That bullying (including cyberbullying) has a negative and often lasting impact on mental wellbeing.
- Where and how to seek support (including recognising the triggers for seeking support), including whom in school they should speak to if they are worried about their own or someone else's mental wellbeing or ability to control their emotions (including issues arising online).

Internet safety and harms

- That for most people the internet is an integral part of life and has many benefits.
- About the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- Why social media, some computer games and online gaming, for example, are age restricted.
- That the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.
- Where and how to report concerns and get support with issues online.

Secondary

In **Key Stage 3** pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.

- Recognise inappropriate content, contact and conduct, and know how to report concerns.

In **Key Stage 4** pupils will be taught to:

- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to identify and report a range of concerns.

By the end of secondary school, pupils will know:

Respectful relationships and friendships

- The characteristics of positive and healthy friendships (in all contexts, including online) including: trust, respect, honesty, kindness, generosity, boundaries, privacy, consent and the management of conflict, reconciliation and ending relationships. This includes different (non- sexual) types of relationship.
- Practical steps they can take in a range of different contexts to improve or support respectful relationships.
- How stereotypes, in particular stereotypes based on sex, gender, race, religion, sexual orientation or disability, can cause damage (e.g. how they might normalise non-consensual behaviour or encourage prejudice).
- That in school and in wider society they can expect to be treated with respect by others, and that in turn they should show due respect to others, including people in positions of authority and due tolerance of other people's beliefs.
- About different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders to report bullying and how and where to get help.
- That some types of behaviour within relationships are criminal, including violent behaviour and coercive control.
- What constitutes sexual harassment and sexual violence and why these are always unacceptable.
- The legal rights and responsibilities regarding equality (particularly with reference to the protected characteristics as defined in the Equality Act 2010) and that everyone is unique and equal.

Online and media

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- the impact of viewing harmful content.
- That specifically sexually explicit material e.g. pornography presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.

Being safe

- The concepts of, and laws relating to, sexual consent, sexual exploitation, abuse, grooming, coercion, harassment, rape, domestic abuse, forced marriage, honour-based violence and FGM, and how these can affect current and future relationships.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

Mental Wellbeing

- How to talk about their emotions accurately and sensitively, using appropriate vocabulary.
- How to recognise the early signs of mental wellbeing concerns.
- common types of mental ill health (e.g. anxiety and depression).
- How to critically evaluate when something they do or are involved in has a positive or negative effect on their own or others' mental health.

Internet safety and harms

- The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on

online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online.

- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of Internet safety in letters or other communications home. Additional information will be shared via the website, newsletters or dissemination of resources.

This policy will be shared with parents, who will be invited to attend online safety events in person or remotely. Queries or concerns should be raised with tutors in the first instance but can be escalated to heads of year, e-safety co-ordinator, strategic leadership team, designated safeguarding leads or the Principal as appropriate. Concerns or queries about this policy can be raised with the e-safety co-ordinator, DSL or Principal.

6. Cyber-bullying

6.1. Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power (see 'Behaviour for Learning' policy for further information).

6.2. Preventing and addressing cyber-bullying

We aim to prevent occurrences of cyber-bullying but ensure that students can identify the signs and are encouraged to report instances involving themselves or others.

The school actively discusses cyber-bullying with pupils, explaining why it occurs, the forms it may take and what the consequences can be. Tutors discuss cyber-bullying with their tutor groups, and the issue is addressed in assemblies. Teaching staff are encouraged to find opportunities to use aspects of the curriculum to

cover cyber-bullying. This includes but is not limited to Computing and Personal, Social, Health and Economic (PSHE) education.

All staff, governors and volunteers receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (See Section 11 for further details).

The school provides information and guidance on cyberbullying which raises the awareness of amongst parents. It is important that they can identify the signs, know how to report it and are empowered to support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police and will work with external services if it is deemed necessary to do so.

6.3. Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for, and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a "good reason" to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm.
- Disrupt teaching.
- Break any of the school rules.

If inappropriate material is found on the device, it is up to the staff member, in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material.
- Retain it as evidence (of a criminal offence or breach of school discipline).
- Report it to the police.

Any searching of pupils will be carried out in line with the DFE's latest guidance on screening, searching and confiscation.

Complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers, board members and governors are expected to accept an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendix 1). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We maintain the right to monitor the websites visited by pupils, staff, volunteers, board members, governors and visitors to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils are permitted to bring mobile devices into school but they must adhere to the Student Code of Conduct, and associated policies (e.g. Network, Internet & Email Acceptable Use Policy).

- Students remain responsible for their devices and should not expect to charge them on-site.
- Devices must remain in silent mode unless otherwise stated.
- Applications or media must be age appropriate.
- Students must not use devices to record, transmit or post photographic images or videos unless instructed by a member of staff.
- School WiFi must be used to access the Internet whilst on site as this is filtered and provides a safer environment in which to surf.
- Use of Virtual Private Networks to circumvent filtering restrictions is strictly prohibited.
- Personal devices should not be used in the transition or movement between lessons.
- The teacher has the sole discretion to allow and regulate the use of personal devices in the classroom.
- The student may only accesses programs or websites as directed.

- Making or responding to phone calls/messages during lessons is not permitted.

St Johns Marlborough takes no responsibility for stolen, lost or damaged devices (including corruption of data).

Any inappropriate use of mobile devices in school by pupils may trigger disciplinary action in line with the school behaviour policy. This may result in the confiscation and/or examination of devices.

9. Staff using school owned devices

Staff members using school owned devices must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager. Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures or guidance set out in our 'Behaviour for Learning' and 'Network, Internet and & Email Acceptable Use' policies. The action taken will be proportionate but depend on the nature or seriousness of the incident.

Staff members who misuse devices, infrastructure, systems or services owned/managed by the school will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances but may result in disciplinary procedures depending on the seriousness of the incident. This can and will include personal devices where the action constitutes misconduct.

The school will consider whether incidents should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (e.g. emails, staff meetings and continuing professional development sessions).

The DSL and deputy/deputies will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in child protection and safeguarding policy.

12. Monitoring arrangements

Teachers possess the ability to log and monitor general e-safety related incidents within Class Charts.

Serious behaviour and safeguarding issues relating to online safety are logged by the DSL in CPOMS.

This policy will be reviewed every year by the Trust and Education Scrutiny Committee.

It will be reviewed on an annual basis locally by the DSL and the review will be shared with the LGB.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary Procedures
- Data protection policy and privacy notices
- Concerns and Complaints procedure
- ICT and internet acceptable use policy
- Excalibur Employment manual
- Anti-Bullying Policy
- Behaviour for Learning Policy
- Relationships and Sex Education Policy

Appendix 1: Acceptable Use Policy for Students

Network, Internet and Email Acceptable Use Policy for Students

Student Name:

I agree to follow the rules below whilst using the school network, devices or services.

Policy Statement

The purpose of this policy is to ensure that users of the St John's computer network fully understand how the Network, Internet and Email are to be used. Specifically, this document aims to ensure that these resources are used for their intended purpose, without infringing legal requirements or creating additional risk. Users should read this policy carefully to ensure that they fully understand the terms of use.

St John's encourages users to make effective use of the computer network in order to support teaching and learning. Whilst these activities are permitted they must always remain lawful, appropriate and avoid creating unnecessary risk or harm to other individuals. Users of the network must not intentionally compromise information stored, create damage to computer systems or tarnish the reputation of St John's.

Please read this policy carefully as you will be deemed to be aware of its contents.

Use of the network, Internet and services

St John's expects all users of the network to be responsible and use its facilities in accordance with the conditions outlined below.

In particular, the following activities are deemed unacceptable:

Seeking to view or distribute inappropriate or illegal material

- Visiting websites that contain illegal, obscene, hateful, discriminatory, radical or pornographic material.
- Creating, storing or distributing images, text or other materials that might be considered indecent, pornographic, discriminatory, hateful, obscene or illegal.
- Promoting any form of discrimination, including racism, sexism or religious hatred.

Cyber-bullying

- Using communications technologies (e.g. text messaging, emails and social networking sites) to torment, threaten, harass, humiliate or target individuals in a hostile manner.
- Creating or storing images, text or other materials that could be potentially insulting or offensive.

Network misuse

- Introducing any form of computer virus into the school network.
- Installing software applications/packages without consent of the Network Manager.

- Making modifications or performing repairs to the network or its equipment.
- Distributing login details to third parties or providing network access to unauthorised users.
- Leaving computers unlocked when the machine is unattended.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Deliberately wasting Network resources such as printers, paper or ink.
- Physically damaging or otherwise interfering with the network or services.
- Consuming food or drink (except bottled water) in computer suites.
- Leaving computer suites untidy.

Copyright violation and fraudulent activities

- Downloading, accessing or distributing data in a way that violates copyright laws.
- Hacking or gaining unauthorised access to accounts/areas on the network.
- Using the computer to commit any form of fraudulent activity or impersonation.

Inappropriate communications and failure to comply with Data Protection

- Sending spam, junk, chain or unsolicited bulk emails.
- Transmitting unsolicited, commercial or advertising material.
- Forwarding confidential messages or information to external locations or parties.
- Broadcasting unauthorised personal views on social, political, religious or academic matters.
- Using communications systems to set up personal businesses or seek commercial gain.
- Failing to comply with the Data Protection Act 1998, GDPR, or the academies Data Protection Policy.

Guidance/protection for Students on use of social networking sites

Social networking sites should not be accessed without prior consent from a member of staff. In the event that these services are being used, there must be a strong educational purpose and steps taken to protect the safety of students. No student should attempt to join a staff member's personal area on social networking sites and requests should not be made or accepted by teachers. Any concerns should be reported in accordance with the online safety policy.

Monitoring

St John's accepts that the use of the Network, Internet & email is a valuable tool. However, misuse of this facility can have a negative impact upon student productivity and the reputation of St John's.

Resources should be used primarily for educational and management purposes. The school maintains the right to monitor the volume and nature of Internet, email and network traffic, together with the Internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Any serious breach will be duly reported and sanctioned in accordance with the Online Safety policy.

Sanctions

Failure to comply with these guidelines will result in sanctions ranging from use of the facilities being withdrawn on a semi-permanent or permanent basis, through to exclusion for students with repeat offences. Offences of a criminal nature, such as copying third party software without a licence or inappropriate communication may lead to prosecution without protection from St John's Marlborough.

Agreement

All users of the St John's network are required to agree to the Network, Internet and Email Acceptable Use Policy before being granted access. It is important to note that this agreement applies to privately owned computer equipment being used on site. The policy also covers wireless and remote connections made to the school network.

I am aware that the school will monitor my actions whilst using IT systems and that there may be consequences if I do not follow the rules.

Signed (Student):	**Date:**

Appendix 2: Acceptable Use Policy for Staff, Governors, Volunteers and Visitors

Network and Internet Acceptable Use Agreement for Staff, Governors, Volunteers and Visitors

Name:

Position:

I will abide by the regulations below whilst using the academies network, devices orservices and understand that these apply when working remotely.

IT Acceptable Use Policy

1. **Introduction**

   This policy sets out the requirements with which you must comply when using the Trust'sIT and when otherwise using IT in connection with your job including:

   - The Trust's email and internet services.
   - Telephones and faxes;
   - the use of mobile technology on Trust premises or otherwise in the courseof your employment (including 3G / 4G, Bluetooth and other wireless technologies) whether using an Academy, Trust or a personal device; and
   - any hardware (such as laptops, printers or mobile phones) or softwareprovided by, or made available by, the Trust.

   This policy also applies to your use of IT off Trust premises if the use involves Personal Information of any member of the Trust community or where the culture or reputationof the Trust or any of its academies are put at risk.

2. **Failure to comply**

   Failure to comply will constitute a disciplinary offence and will be dealt with under theTrust's Disciplinary Procedure.

3. **Property**

   You should treat any property belonging to the Trust with respect and reasonable care and report any faults or breakages immediately to your line manager. You should not usethe Trust's computers or other IT resources unless you are competent to do so and should ask for training if

you need it.

4. Viruses and other malicious code

You should be aware of the potential damage that can be caused by computer viruses andother malicious code. You must not introduce or operate any hardware, software, code/script or data, additionally suspicious emails which have not first been checked by the Trust for viruses should not be opened.

5. Passwords

Passwords should be long, for example you could use a song lyric or a memorable phraseplus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else. In addition:

- Your password should be difficult to guess, for example you could base yourpassword on something memorable that no one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.
- You must not use a password which is used for another account. For example, you must not use your password for your private email address oronline services for any school account.
- Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not beshared with, or given to, anyone else. Passwords should not be written down.

6. Leaving workstations

If you leave your workstation for any period of time you should take appropriate action and, in particular, you should log off or lock your device so that a password is required togain access again.

7. Concerns

You have a duty to report any concerns about the use of IT at the Trust to a seniorcolleague. For example, if you have a concern about IT security or pupils accessing inappropriate material.

8. Other policies

This policy should be read alongside the following:

- Code of Conduct

- Data Protection policy for Staff
- Information Security Policy
- Acceptable Use Policy for Students.

Internet:

9. Downloading

Downloading of any programme or file which is not specifically related to your job isstrictly prohibited.

10. Personal use

The Trust permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right.If the Trust discovers that excessive periods of time have been spent on the internet provided by the Trust or it has been used for inappropriate purposes (as described in section 14 below) either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Principal.

11. Unsuitable material

Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the Trust believes is unsuitable, at any time, is strictly prohibitedand constitutes gross misconduct. Internet access may be withdrawn without notice at the discretion of the Head whilst allegations of unsuitable use are investigated by the Trust.

12. Location services

The use of location services represents a risk to the personal safety of those within theTrust community, the Trust's security and its reputation. The use of any website or application, whether on a Trust or personal device, with the capability of publicly identifying the user's location while on Trust premises or otherwise in the course of employment is strictly prohibited at all times.

13. Contracts

You are not permitted to enter into any contract or subscription on the internet (including through an App) on behalf the Trust or any of its Academies, without specificpermission from the Principal. This applies both to "free" and paid for contracts, subscriptions and Apps.

14. Retention periods

The Trust keeps a record of staff browsing histories for a period of 30 days.

Email:

15. Personal use

The Trust permits the incidental use of its email systems to send personal emails as longas such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled 'personal' in the subject header. Use must notinterfere with your work commitments (or those of others). Personal use is a privilege and not a right. The Trust may monitor your use of the email system, please see paragraphs 26 to 30 below, and staff should advise those they communicate with that such emails may be monitored. If the Trust discovers that you have breached these requirements, disciplinary action may be taken.

16. Status

Email should be treated in the same way as any other form of written communication.Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published generally.

17. Inappropriate use

Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwisecontrary to our equal opportunities policy), or defamatory is not permitted. Use of the email system in this way constitutes gross misconduct. The Trust will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.

18. Legal proceedings

You should be aware that emails are disclosable as evidence in court proceedings andeven if they are deleted, a copy may exist on a back-up system or other storage area.

19. Jokes

Trivial messages and jokes should not be sent or forwarded to the email system. They could cause the Trust's IT system to suffer delays and / or damage or could cause offence.

20. Contracts

Contractual commitments via an email correspondence are not allowed without priorauthorisation of the Principal.

21. Disclaimer

All correspondence by email should contain the Trust's disclaimer.

22. Data protection disclosures

Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a subject access request under data protection legislation. There is no exemption for embarrassing information (for example,an exchange of emails containing gossip about the individual will usually be disclosable).

Staff must be aware that anything they put in an email is potentially disclosable.

Monitoring:

23. The Trust regularly monitors and accesses its IT system for purposes connected with theoperation of the Trust. The Trust IT system includes any hardware, software, email account, computer, device or telephone provided by the Trust or used for Trust business. The Trust may also monitor staff use of the Trust telephone system and voicemail messages. Staff should be aware that the Trust may monitor the contents of a communication (such as the contents of an email).

24. The purposes of such monitoring and accessing include:

- To help the Trust with its day to day operations. For example, if a memberof staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received.
- To check staff compliance with the Trust's policies and procedures and to help the Trust fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to sendabusive or inappropriate messages.

25. Monitoring may be carried out on a random basis and it may be carried out in responseto a specific incident or concern.

26. The Trust also uses software which automatically monitors the Trust IT system (for example, it would raise an alert if a member of Staff visited a blocked website or sent anemail containing an inappropriate word or phrase).

27. The monitoring is carried out by The Trusts IT personal or a company contracted to provide the Trust with ICT services and support. If anything of concern is revealed as aresult of such monitoring then this information may be shared with the schools Principal and other senior staff where necessary and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such asthe Police.

I will:

- Only use the school's ICT systems and access the internet in school, or outside school ona work device, for educational purposes or for the purpose of fulfilling duties of my role.
- Take all reasonable steps to ensure that work devices are secure and password-protectedwhen using them outside school, and keep data securely stored in accordance with this policy and the school's data protection policy.
- Let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and willalso do so if I encounter any such material.
- Always use the school's ICT systems and internet responsibly and ensure that pupils inmy care do so.

I will not:

- Access, or attempt to access inappropriate material, including but not limited to materialof a violent, criminal or pornographic nature (or create, share, link to or send such material).
- Use them in any way which could harm the school's reputation.
- Access social networking sites or chat rooms.
- Use any improper language when communicating online, including in emails or othermessaging services.
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network.
- Share my password with others or log in to the school's network using someone else's details.
- Take photographs of pupils without checking with teachers first.

- Share confidential information about the school, its pupils or staff, or other members ofthe community.
- Access, modify or share data I'm not authorised to access, modify or share.
- Promote private businesses, unless that business is directly related to the school.

I am aware that the school will monitor my actions whilst using IT systems and that there may be disciplinary action if I do not follow the rules.

Signature:	**Date:**