POLICY:
Online Safety

Review

Approved by:	Board of Directors	**Date:**	April 2024
Last Review Date:	April 2024	**Next Review Date:**	April 2025

Responsibilities

School Senior Staff	Implementation at school level
Governors	Check school compliance with policy and report breaches or concerns to Directors
Directors	Review and approve the processes/procedures

Material Changes Since the Last Review

Section: Throughout	Name change from Kennet School Academies Trust to Equinox Learning Trust

Contents

1. Aims 2
2. Roles & Responsibilities 2
3. Educating Pupils about Online Safety 4
4. Educating Parents/Carers about Online Safety 5
5. Cyber-bullying 5.1 Definition 5
6. Acceptable use of the Internet in School 6
7. Pupils using Mobile Devices in School 7
8. Staff Using Work Devices Outside School 7
9. How the School Responds to Issues of Misuse 7
10. Training 7
11. Monitoring Arrangements 8
12. Links with Other Policies 8
Appendix A 9
Appendix B 12
Appendix C 17

1. Aims

The Equinox Learning Trust aims to:

- Safeguard and protect all members of the Trust community online
- Identify approaches to educate and raise awareness of online safety throughout the whole community
- Establish clear procedures to identify, intervene and escalate an incident, where appropriate.

This policy takes into account the guidance from the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2022, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and Cyber-bullying: advice for Headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 2011, the Education and Inspections Act 2006 and the Equality Act 2010. This includes given teachers' 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 a 'good reason' to do so.

The policy also considers the National Curriculum computing programmes of study and complies with our funding agreement and articles of association.

- The Trust identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
- **Content:** being exposed to illegal, inappropriate, or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

Equinox Learning Trust believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all members of the school community are protected from potential harm online. It identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. The Trust believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers, and other individuals who work for, or provide services on behalf of the Trust (collectively referred to as "staff" in this policy) as well as pupils, parents/carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets, or mobile phones.

2. Roles & Responsibilities

The Equinox Learning Trust recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

2.1 The Governing Board

The Board of Directors have overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

- Each Local Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safeguarding logs as provided by the designated safeguarding lead (DSL)
- The Governors who oversee Safeguarding can be found on the individual school websites.

All directors/governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix C)
- Ensure that online safety is embedded within a progressive curriculum, which enables all pupils to develop an age-appropriate understanding of online safety

2.2 The Headteacher

The Headteacher will:

- Ensure staff understand this policy
- Ensure the policy is being implemented consistently throughout the school
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local guidance
- Ensure online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches
- Ensure there are appropriate and up-to-date policies regarding online safety; including a behaviour policy, which covers acceptable use of technology.

2.3 The Designated Safeguarding Lead (DSL)

Details of the school's DSL and Deputy DSL are set out in our Child Protection & Safeguarding Policy as well relevant job descriptions.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, Network Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring up-to-date staff training and support on online safety, particularly for SEND pupils who are at an additional risk (appendix 4 contains a self-audit for staff on online safety training needs)
- Monitor online incidents to identify gaps and trends, and use this information to update the education response, policy and procedures in the school
- Ensuring that any online safety incidents and actions are logged, as part of the school's safeguarding policy 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
- Liaising with other agencies and/or external services, as appropriate
- Providing regular reports on online safety in school to the Headteacher and/or governing board to support the review and update of the online safety policy on a regular basis (annually)

This list is not intended to be exhaustive.

2.4 The Network Manager

The ICT /Network Manager is responsible for:

- Implementing appropriate safety measures, as directed by the DSL and leadership team, such as password policies and encryption, to ensure that the trust's IT infrastructure/system is secure whilst maximising learning opportunities
- Putting in place appropriate filtering and monitoring systems (which are regularly updated) to keep pupils safe from potentially harmful and inappropriate content and contact online while at school
- Ensuring that the trust's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Conducting a full security check and monitoring the trust's ICT systems takes place routinely and security monitoring systems run all the time.

This list is not intended to be exhaustive.

2.5 All Staff & Volunteers
All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix C) and ensuring that pupils follow the school's terms on acceptable use (appendices A or B)
- Working with the DSL to ensure 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 line with the school behaviour policy

This list is not intended to be exhaustive.

2.6 Parents/Carers
Parents/Carers are expected to:

- Ensure their child has read, understood, and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices A or B)
- Support the school's online safety approaches by discussing online safety issues with their children and reinforce appropriate and safe online behaviours at home and in school
- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Seek help and support from the school, or other appropriate agencies, if they or their child encounters risk or concerns online.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet Childnet Internationl

2.7 Visitors & Members of the Community
Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

3. Educating Pupils about Online Safety

Trust schools has strong coverage of online safety in their PSHE and wider curriculum to raise awareness and promote safe and responsible internet use amongst pupils.

Pupils will be taught about online safety through:

- E-safety in Personal, Social, Health Education PSHE) through our tutorial programme, Relationship and Sex Education (RSE) and Religious Studies and Computing programmes of study
- In primary schools, pupils will also be taught through the Relationships education and health education

Whitelands Park/Francis Baily Primary Schools:
In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping 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

Pupils in **Key Stage 2** 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:*

- 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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Kennet School:
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** will be taught:
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns.

*By the **end of secondary school**, they will know:*
- 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
- 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.

4. Educating Parents/Carers about Online Safety
The Equinox Learning Trust recognises that parents/carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies. We build a partnership approach to online safety with parents/carers by:
- Providing information and guidance on online safety in a variety of formats (letters or other communications home, and in information via our website)
- Sharing this policy with parents/carers
- Requiring them to read our acceptable use policies and discuss the implications with their children
- In Kennet School, parents/carers will also be invited to attend an Online safety event in the Autumn Term.
- In Primary settings, each school will provide safety sessions every other year.

5. Cyber-bullying
5.1 Definition
Cyber-bullying takes place online, including sending offensive, upsetting, degrading and inappropriate messages, videos or photos by phone, text, instant messenger, through social networking sites or apps, 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 also the each school's behaviour policies.

5.2 Preventing & Addressing Cyber-bullying
The Trust is committed to ensuring all members of our community are safe from bullying. To help prevent cyber-bullying we will:

- Actively discuss cyber-bullying with pupils, explaining what it is, the reasons why it occurs, the forms it may take and the consequences. Members of the pastoral team will discuss cyber-bullying with pupils through the tutorial programme and assemblies
- Educate pupils in E-safety through Personal, Social, Health and Economic (PSHE), Relationship and Sex Education (RSE) and Religious Studies and Computing programmes of study
- ensure that pupils understand what to do if they become aware of it happening to them or others.
- ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim
- ensure we follow the processes set out in each school's Behaviour Policy when dealing with an incident. 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 if it involves illegal material and will work with external services if it is deemed necessary to do so
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see Section 10 for more detail)

5.3 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, and/or
- Disrupt teaching, and/or
- 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, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- 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.

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

6. Acceptable use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use when using a computer.

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 will monitor the websites visited by pupils, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in Appendices 1, 2 and 3.

7. Pupils using Mobile Devices in School

- In Primary School, Year 5 and 6 pupils may bring mobile devices into school if they travel to and from school unaccompanied but must turn them off and leave them at the school office during the day. They collect them after 3.15pm for their journey home
- In Kennet School, not allowed to have mobile phones on them during the day. If they need them for safe travel to and from school, they must be turned off and stowed in their bags during the day. If seen, regardless of use, they will be confiscated and returned in line with the appropriate sanction level

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's Behaviour Policy, which will result in the confiscation of their device.

8. Staff Using Work Devices Outside School

Staff members using a work device outside school 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 3.

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 ICT/Network Manager. Work devices must be used solely for work activities.

9. How the School Responds to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Child Protection and Safeguarding, Behaviour and ICT and internet acceptable use). The action taken will depend on the individual circumstances, nature, and severity of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature, and severity of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. 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 (for example through emails, e-bulletins and staff meetings). The DSL and Deputy DSL 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 about 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, as applicable.

More information about safeguarding training is set out in the Trust's Child Protection & Safeguarding Policy.

11. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This policy will be reviewed every year by the Deputy Headteacher (Pastoral). At every review, the policy will be shared with the governing board.

12. Links with Other Policies

This online safety policy is linked to our:

- Child Protection & Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- Acceptable Use Policies
- Staff Social Media Policy

You can find all our policies on our website.

Appendix A: EYFS, Key Stages 1&2 acceptable use agreement (Pupils & Parents/Carers)

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended toensure:

- that the pupils in our school will be responsible users and stay safe while using the internet and other digital technologies for educational, personal, and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety

- I understand that the staff at my School will monitor my use of the systems, devices, and digital communications
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will be aware of "stranger danger" when I am communicating online
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, etc)
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take an adult with me
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online

I understand that everyone has equal rights to use technology as a resource and:

- I understand that School systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions
- I will not take or distribute images of anyone without their permission

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will immediately report any damage or faults involving equipment or software; however, this may have happened
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form
This form relates to the pupil acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) eg mobile phones, USB devices, etc
- I use my own equipment out of the school in a way that is related to me being a member of this school, eg communicating with other members of the school, accessing school email, use of Zoom/Google Classroom, website etc

Pupil

Name of Pupil:	**Tutor Group:**
Signed:	**Date:**

Parent/Carer Countersignature

Signed:	**Date:**

Appendix B: Acceptable Use Agreement (Kennet School Pupils & Parents/Carers)

Why have an Acceptable Use Policy?

An Acceptable Use Policy is about ensuring that you, as a pupil at Kennet School can use the internet, email and other technologies available at the school in a safe and secure way. The policy also extends to out of school facilities, eg equipment; printers and consumables; Internet and email; managed learning environments and websites.

An Acceptable Use Policy also seeks to ensure that you are not knowingly subject to identity theft and therefore fraud. Also, that you avoid cyber-bullying and just as importantly, you do not become a victim of abuse. We have also banned certain proxy sites as well as anonymous proxy sites because they put the school network at risk. Help us, to help you, keep safe.

Kennet School recognises the importance of ICT in education and the needs of its pupils to access the computing facilities available within the school. The school aims to make the ICT facilities it has available for pupils to use for their studies both in and out of lesson times.

Listed below are the terms of this agreement. All Kennet pupils are expected to use the ICT facilities in accordance with these terms. Violation of terms outlined in this document may lead to loss of access and/or disciplinary action, which will be taken in accordance with the school's Behaviour Policy.

Equipment

Vandalism

Vandalism is defined as any action which harms or damages any equipment or data that is part of the school's ICT facilities and is deemed completely unacceptable. Such vandalism is covered by the Computer Misuse Act 1990 (see Glossary). This includes, but is not limited to:

- Deliberate damage to computer hardware such as monitors, base units, printers, keyboards, mice or other hardware
- Change or removal of software
- Unauthorised configuration changes
- Creating or uploading computer viruses
- Deliberate deletion of files

Such actions reduce the availability and reliability of computer equipment and puts at risk other users' data. In addition, these actions lead to an increase in repairs of the ICT facilities, which impacts upon every pupil's ability to use the ICT facilities. The other result of vandalism is that it incurs cost, which reduces the funds available to improve the ICT facilities the school has. Should you be found to have damaged equipment, you will be expected to re-imburse the school for the repairs or replacement of equipment.

Use of Removable Storage Media

Due to Data Protection Act, removable storage media is prohibited, and the school's systems are set up to stop pupils using them. However, the school accepts the fact that pupils may wish to transfer schoolwork from home to school, we therefore encourage you to use the "My Documents and Shared Files" section of Frog, or email, when transferring work between home and school. For larger files, such as video and photography, external cloud services, such as OneDrive, as well as others, can be used but only OneDrive is officially supported by the school. Guidance must first be sought from the IT Department.

Printers & Consumables

Printers are provided in the school's library for use by pupils. Please use the printers sparingly and for educational purposes only. Take the time to check the layout and proofread your work using the 'Print Preview' facility before printing.

All printer use is recorded and monitored and therefore if you deliberately use the printer for non-educational or offensive material, disciplinary action which will be taken in accordance with the schools' Behaviour Policy.

Data Security & Retention

All data stored on the Kennet School's network is backed up daily and backups are stored for two weeks. If you should accidentally delete a files or files in your folder or shared area, please inform a member of the IT Department immediately so that it can be recovered. Generally, it is not possible to recover files that were deleted more than two weeks previously.

Internet & Email

Content Filtering

Kennet School provides internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you come across any inappropriate website or content whilst using the ICT equipment, you must report it to a member of staff immediately.

The use of Internet and email is a privilege and inappropriate use will result in that privilege being withdrawn.

Acceptable use of the Internet

All Internet access is logged and actively monitored, and details are stored for two months and usage reports can and will be provided to any member of staff upon request.

Use of the Internet should be in accordance with the following guidelines:

- Only access suitable material – the Internet is not to be used to download, send, print, display or transmit material that would cause offence or break the law
- Do not access Internet Chat sites. Remember you could be placing yourself at risk
- Never give or enter your personal information on a website, especially your home address, your mobile number or passwords
- Online games websites should not, under any circumstances, be accessed during lesson times and may only be used during supervised lunch-time clubs, if applicable
- Do not download or install software from the Internet, as it is considered to be vandalism of the school's ICT facilities
- Do not use the Internet to order goods or services from on-line, e-commerce or auction sites
- Do not subscribe to any newsletter, catalogue, or other form of correspondence via the Internet
- Do not print pages directly from a website. Web pages are often not properly formatted for printing, and this may cause a lot of waste. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting

Email

Pupils will be provided with an email address by the school, and the expectation is that you will use this facility for legitimate educational and research activity only and not register for any personal site including social media.

During lessons email should only be used when instructed by your teacher, and for educational purposes only. Email can also be accessed during your own social time but please carefully follow the guidelines laid out below.

You are expected to use email in a responsible manner. The sending or receiving of messages which contain any material that is of a sexist, racist, unethical, illegal, or likely to cause offence should not take place.

Remember when sending an email to:

- Be polite - never send or encourage others to send abusive messages.
- Use appropriate language - remember that you are a representative of the school on a global public system. What you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language
- Do not reveal any personal information about yourself or anyone else, especially home addresses, personal telephone numbers, usernames or passwords. Remember that electronic mail is not guaranteed to be private
- Consider the file size of an attachment. Files exceeding 10MB in size are generally considered to be excessively large and you should consider using other methods to transfer such files. Speak to a member of the IT Department for advice
- Do not download or open file attachments unless you are certain of both their content and origin. File attachments may contain viruses that may cause loss of data or damage to the school network

Cyber-bullying

In the event of a cyber-bullying incident the same procedures will be followed as for all other incidents of poor behaviour (see Behaviour Policy on our website). In all cases details of the incident and action taken will be recorded.

External Services

Office 365

Office 365 provides remote access to your email account from home or anywhere with an Internet connection. Use of this service is subject to the following guidelines. Use of the facility is closely and actively monitored, and any abuse or misuse will result in the facility being withdrawn and/or other disciplinary action being taken against you.

- Office 365 is provided for use of Kennet School staff and pupils only. Access by any other person is not allowed
- Never reveal your password to anyone
- Remember to treat file attachments with caution. File attachments may contain viruses that may cause loss of data or damage to the computer from which you are working. Do not download or open file attachments unless you are certain of both their content and origin. Kennet School accepts no responsibility for damage caused to any external equipment or software, as a result, of using the Office 365 service

Managed Learning Environment Software

FROG, Kennet School's Virtual Learning Environment (VLE) provides a web-based portal allowing users access to personalised learning resources and lesson materials. Use of this service should only be in accordance with instructions from your subject tutor and in accordance with the following guidelines:

- The VLE is provided for use of Kennet School staff, pupils, and parents (although parents have more restricted access to content). Access by any other party is strictly prohibited
- Never reveal your password to anyone or attempt to access the service using another pupil's login details
- FROG is provided by Frog Education and Kennet School can make no guarantees as to service availability or quality

Social Networking & File Sharing Sites

Whilst accessing social networking sites (Instagram, LinkedIn, Facebook, etc) is restricted within the school environment, we appreciate the large number of pupils who will be using this in free time outside of school. Please bear in mind that including any details about the school you attend on your profile not only introduces a very serious safety risk, it also makes you a representative of the school. As such, we strongly recommend you do not post any such details to any social networking sites. Any behaviour which could bring the school into disrepute may result in computer access being restricted and further disciplinary action being taken.

The uploading of any photos or videos taken within school grounds or containing any other pupils or a member of staff without their consent is not allowed under any circumstance.

Privacy

Passwords

- Never share your password with anyone else or ask others for their password
- When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name or address. Generally, longer passwords are better than short passwords
- If you forget your password, inform a member of the IT Department immediately who will help you reset it
- If you believe that someone else may have discovered your password, then change it immediately and inform a member of staff

Security

- Never attempt to access files or programs to which you have not been granted access to. Attempting to bypass security barriers may breach Data Protection Regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action
- You should report any security concerns immediately to a member of staff
- If you are identified as a security risk to the school's ICT facilities, you will be denied access to the systems and be subject to disciplinary action

Storage & Safe Transfer of Personal Data

Kennet School holds information on all pupils and in doing so, we must follow the requirements or the Data Protection Act 2018 (see Glossary). This means that data held about pupils can only be used for specific

purposes and therefore all data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018 – see the school's Pupil Privacy Policy available on the school website.

Service

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the school will not be responsible for any damages or loss incurred because of system faults, malfunctions, or routine maintenance. These damages include loss of data as a result of delay, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the school's ICT facilities is at your own risk. Kennet School specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

Mobile Technology

Acceptable Use of Mobile Devices

For reasons of safety and security pupils should not use their mobile phone or any other technology in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person.

The development of mobile technology is such that mobile phones and other similar devices connected to mobile networks have enhanced features which include picture messaging; mobile access to the Internet; entertainment in the form of video streaming and downloadable video clips from films, sporting events, music and games.

If you are sent inappropriate material, eg images or videos report it immediately to a member of staff within the school.

Mobile Phones

If mobile telephones are brought into school, they must be switched off and kept in your bags at all times to ensure they cause no disruption to teaching and learning. The only exception is for Sixth Form pupils who are permitted use their mobile phones in the Sixth Form block. If a Year 7-11 pupil is found using their phone during school hours, the following procedure will take place:

- Confiscation by the teacher/member of staff with no argument from the pupil (you know the rules)
- The mobile phone will be handed to the pupil's Head of House
- The pupil will have to see the Head of House at the end of the day to get their mobile phone back
- The Head of House will keep a record of phones that have been confiscated
- If a pupil's phone is confiscated for a second time in a year, it will not be returned that evening but the following evening
- If a pupil's phone is confiscated for a third time in a year, it will be kept for a week and then the pupil's parents will be asked to collect the mobile phone in person – it will not be handed to the pupil at that point
- The school, its staff and governing body takes no responsibility for loss or theft of any mobile phones which pupils choose to bring into school

Tablet PCs & Notebooks

Kennet School strongly advises pupils to leave any high value devices at home as correct and appropriate ICT facilities will be provided whenever necessary. However, we recognise that our Sixth Form students may wish to do so. Any devices which are brought into school must be used appropriately and responsibly. The school, its staff and governing body takes no responsibility for loss or theft of any Tablet PC's and Notebooks which Sixth Formers choose to bring into school.

Glossary

Computer Misuse Act (1990)

The Computer Misuse Act makes it an offence for anyone to have unauthorised:

- access to computer material e.g., if you find/guess another pupil's password and use it
- access to deliberately commit an unlawful act, eg if you guess a fellow pupil's password and access their learning account without permission
- changes to computer material, eg if you change the desk-top set up on your computer or introduce a virus deliberately to the school's network system

Data Protection Act (2018)
The Data Protection Act ensures that information held about you is used for specific purposes only. These rules apply to everyone in the school, including teaching staff, support staff, volunteers, and governors.

The Act covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the school. The Act not only applies to paper files it also applies to electronic files.
The principles of the Act state that data must be:

- Processed lawfully, fairly and in a transparent manner
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept no longer than necessary
- Secure
- Not transferred to other countries without adequate provision

RIPA – Regulation of Investigatory Powers Act (2000)
If a request for authorised access is made to the school, Kennet School will provide the appropriate access to your ICT records and files. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for:

- the interception of communications
- the acquisition and disclosure of data relating to communications
- the carrying out of surveillance
- the use of covert human intelligence sources
- access to electronic data protected by encryption or passwords

Appendix C: Acceptable Use Agreement (Staff, Governors, Volunteers & Visitors)

Staff (and Volunteer) Acceptable Use Policy Agreement
New technologies have become integral to the lives of children and young people today, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should always have an entitlement to safe access to the internet and digital technologies.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work. The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety

- I understand that the school will monitor my use of the school digital technology and communications systems
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g., laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are intended for educational use and that I will not use the systems for personal or recreational use
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to the appropriate person

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured
- I will not use school systems to access social networking sites
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any online activity that may compromise my professional responsibilities

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses
- I will not use personal email addresses on the school ICT systems
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will understand that my data is regularly backed up by our IT provider
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity or DFS storage and prevent other users from being able to carry out or save their work
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School GDPR Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)

I understand that I am responsible for my actions in and out of school:

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/directors and/or the Local Authority and in the event of illegal activities the involvement of the police

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

It should be understood that this Acceptable Use Policy Agreement is in place to protect adults in contact with children from potential risk in their use of ICT in their everyday work.

The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may have taken place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

I confirm that I have read and understood the Acceptable Use Policy for ICT and agree to abide by it. I understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from the ICT team.

Signed:	**Date:**
Print Name:	