

The Family of Learning Trust

Cyber Security Policy



**This policy is non contractual and may be updated or changed by the Trust
subject to consultation (if required)**

Version	01/26
Name of Policy Writer	Shameem Hussain/Educate HR
Last Reviewed	June 2026
Next Review Due	June 2027*

***This policy will not expire once the nominal review date is reached, it remains active until
superseded by an updated version**

Contents	Page
1. Introduction.....	3
2. Purpose and scope	3
3. Individual roles and responsibilities.....	4
4. Curriculum.....	6
5. Managing the ICT infrastructure	7
6. School website.....	9
7. Use of ICT equipment at home.....	9
8. Use of digital and video photographic images	10
9. CCTV and monitoring	11
10. Other policies and procedures.....	11
 Appendix 1: Staff Acceptable Use Policy on E-safety	 12
Appendix 2: Pupil Acceptable Use Policy on E-safety	16
Appendix 3: E-safety Loan Agreement – Staff	20
Appendix 4: E-safety Loan Agreement – Pupils	21

1. Introduction

- 1.1 The aim of this policy is to set out key principles and expectations for all members of the school community in relation to the use of ICT-based technologies including mobile phones and tablets.. We are committed to safeguarding and promoting the welfare of pupils in line with Keeping Children Safe in Education (KCSIE). Online safety is an integral part of our safeguarding responsibilities, ensuring children can use technology safely and responsibly.
- 1.2 The relevant technologies to which the policy is applicable include, in addition to computers and associated hardware, all electronic devices including (but not limited to) mobile phones, games consoles, cameras and webcams.
- 1.3 In respect of interaction with pupils, management will assist staff to work safely and responsibly when utilising the internet and other communication technologies by supporting them in monitoring their own standards and practice.
- 1.4 There are clear structures in place to minimise the risk of misplaced or malicious allegations made against staff who work with pupils, and also to deal with internet-related issues such as online abuse (including cyberbullying and sexting – defined as sending and/or receiving personally intimate images) and related topics such as identity theft, including ‘frape’ (hacking of facebook profiles).
- 1.5 Ofsted describes e-safety (in relation to schools and academies) as the ability to protect and educate pupils and staff in their use of technology whilst at the same time having appropriate mechanisms in place to intervene and address any incident as and when necessary.
- 1.6 This policy will be communicated to staff and pupils (and the wider community as and when appropriate) via school classrooms/staff rooms and website and will be an integral part of the school induction pack for new staff.
- 1.7 All members of staff in the academy are encouraged (as indeed is the wider community) to exercise vigilance and to be proactive in reporting issues, in the confidence that such concerns will be dealt with quickly and sensitively through the academy’s escalation processes.

2. Purpose and scope

- 2.1 This policy is applicable to all members of our school community who have access to school ICT systems, both on and off school premises. This may include external contractors, trainees, volunteers, parents or carers, visitors, and community users in addition to staff and pupils.
- 2.2 The following extract (in relation to cyber-bullying) is taken from the DfE publication ‘Preventing and tackling bullying: Advice for headteachers, staff and governing bodies’ (July 2017):

The Education Act 2011 amended the power in the Education Act 1996 to provide that when an electronic device, such as a mobile phone, has been seized by a member of staff who has been formally authorised by the headteacher, that staff member can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person’s mobile phone.
- 2.3 The principle of protecting pupils includes the provision of a safe learning environment by use of appropriate monitoring and filtering to control what may legitimately be accessed by

pupils whilst at school. Essentially, however, this only protects them whilst they are on school premises. Ensuring provision of appropriate education relating to e-safety is the only way to guarantee that, irrespective of their whereabouts, they know how to stay safe online.

- 2.4 The aim of this policy (and indeed of our academy) is both to provide appropriate safeguards and to raise awareness to enable pupils (and others) to control their online experiences and thereby feel confident and secure in their use of technology. The entire school community needs to be fully aware of the risks (as well as the undoubted benefits) of information technology and accordingly must undertake to use it in a responsible manner.
- 2.5 Appropriate documents to serve as 'Acceptable Use Policies' (AUPs) and Loan Agreements have been developed which detail the ways in which the internet should be used and such policies (presented in this policy as appendices) are designed to be signed, as and when this might be deemed appropriate, by pupils, their parents/carers, and/or relevant members of staff.
- 2.6 Pupils will be instructed in the acceptable use of ICT at school and will be given clear and principled advice and guidance for general use of mobile technologies including the internet. Appropriate objectives are made clear in the student AUPs and are displayed around the school, particularly where internet access is most frequent, such as in computer suites.
- 2.7 The school will ensure that ICT and information stored electronically will be protected against unauthorised access as well as Information, in particular personal data, is kept confidential. Regulatory and legislative requirements are complied with and ICT security or data protection training is made available to all staff.
- 2.8

3. Individual roles and responsibilities

3.1 Headteacher (Safeguarding Lead)

- to take overall responsibility for the provision of e-safety
- to ensure the school uses an approved, filtered internet service, which is fully compliant with current statutory requirements
- to be responsible for ensuring that all staff receive suitable training to carry out their e-safety roles
- to be responsible for ensuring that any new members of staff are aware of the requirements of this policy and that they have read and signed the staff ICT Acceptable Use policy
- In accordance with the School's financial regulations, shall ensure that an inventory of all ICT equipment is maintained and that all items are accounted for; this review should take place at least once in the school year
- Only authorised personnel who have agreed to use ICT systems in compliance with the school's ICT policies should be allowed access to the ICT systems. **If a staff member, volunteer or other authorised person has failed to sign the Acceptable Use policy then they should not be permitted to use the ICT systems until they have read and signed to agree that they will comply with that policy.**
-
- to ensure that robust systems are in place to monitor and support staff (such as school network manager) who carry out internal e-safety procedures.

- to have day to day responsibility for e-safety issues and to perform a leading role in establishing and reviewing the school's e-safety policy
- to promote awareness and commitment to e-safeguarding throughout the school community
- to ensure that all staff are aware of procedures that need to be followed in the event of an e-safety incident (including completion of an incident log)
- to regularly update their own knowledge and understanding of e-safety issues and legislation (and to cascade this to other staff) and remain constantly aware of the potential for serious child protection issues
- to liaise with the local authority and relevant agencies as appropriate.

3.2 Governor

- to ensure that the school follows all authoritative e-safety advice to protect the welfare of pupils and staff
- to approve the e-safety policy and regularly review the effectiveness of this policy
- to support the school in encouraging parents and the wider community to become engaged in e-safety activities
- to undertake appropriate training and development on e-safety issues.

3.3 IT/ Network Manager

- to report promptly to the e-safety coordinator any related issues that may arise
- to ensure that users may only access the school's network through an authorised password reinforced by a robust and properly enforced protection policy
- to ensure that provision exists for both detection of misuse and protection against malicious attack (for instance by keeping virus protection up to date)
- should be responsible for the level of password control required depending on the nature of the system and the data used/stored on that system.
- to ensure the overall security of the school ICT system such as maintaining the integrity of the data, producing the requisite back up copies of data and protection of the physical access to systems and data.
- to ensure that the adequate security measures are put in place to protect rooms containing ICT equipment (including the server and any cabling). If possible, only authorised personnel should be allowed access to rooms containing servers; if this is not possible then adequate security measures need to be in place to protect servers. The server room should be locked when unattended.
- Access to the internet for children should be filtered using an approved system. It is the responsibility of the ICT manager to monitor effectiveness of the filtering system and report any issues, including breaches or suspected breaches, to the Headteacher.
- To ensure that access controls/encryption are in place to protect all personal and/or sensitive information held on school-owned devices.

3.4 The Data Protection Officer (DPO):

- is responsible for ensuring that the policy is being adhered to in order to comply with the data security requirements and current data protection law
- ensuring staff receive data protection training at least once a year and on induction
- Annual audit take place to identify any areas of weakness

3.5 Staff

- to be aware of e-safety issues related to the use of mobile phones, cameras and other handheld devices and to monitor their use of such devices to ensure compliance with current school policies
- to report any suspected abuse or breach of policy to the DSL
- to maintain an awareness of current e-safety issues, skills development and guidance, for instance through CPD
- ensure the physical security, data security, their password security and that their work is protected/backed up at all times
- to notify the Headteacher and DPO of any suspected or actual breach of the ICT security.
- to model safe, responsible and professional behaviours in their personal use of information technology
- All ICT systems should be protected by passwords and/or screen saver protection
- to read, understand and help promote the school's e-safety policy and related guidance by signing and adhering to the school's 'Staff Acceptable Use Policy' (Appendix 1).

3.6 Pupils

- to understand the importance of reporting abuse, misuse or access to inappropriate materials or sites
- to know what action to take if they or someone they know feels worried or vulnerable when using online technology
- to have a good understanding (appropriate to their age and abilities) of research skills and the need to avoid plagiarism and uphold copyright regulations
- to read, understand, sign* and adhere to the Student Acceptable Use Agreement.

3.7 Parents/Carers

- to support the school in promoting e-safety
- to consult with the school if they have any concerns about their children's use of technology
- to read, understand, sign* (on behalf of their children) and adhere to the Student Acceptable Use Agreement.

****Each school should give careful consideration to setting their own guidelines as to the appropriate age level at which a student's agreement and signature may be considered acceptable either with or without accompanying parental agreement and signature on their behalf.***

4. Curriculum

- 4.1 The academy provides repeated opportunities (within a broad range of curriculum areas) to learn about e-safety. Before accessing the internet for educational purposes pupils will be made aware of the relevant legislation such as data protection and intellectual property rights.
- 4.2 Pupils are also given advice if they experience problems whilst using the internet and/or email and are provided with guidance on promoting e-safety including the requirements to:

- understand the importance of misuse (including accessing inappropriate materials or sites) and be aware of the consequences of this
- understand how to ensure their privacy settings are appropriately configured and to know why they should not post (or share) detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos etc
- understand why they must not post pictures or videos of others without their express consent
- understand issues around plagiarism and how to check copyright etc
- know not to download any files (such as music files) without appropriate permission
- only use approved class email accounts under supervision by (or with permission from) a teacher.

4.3 We recognise the risks children may encounter online fall under the **4Cs framework**:

1. **Content** – being exposed to harmful or inappropriate material (e.g., violence, pornography, extremist content, misinformation).
 - Filtering and monitoring systems are in place.
 - Curriculum teaching includes recognising reliable information and reporting harmful content.
2. **Contact** – being subjected to harmful online interaction with others (e.g., grooming, cyberbullying, online abuse).
 - Pupils are taught not to share personal information and how to report concerns.
 - Staff are trained to recognise and respond to online safeguarding risks.
3. **Conduct** – personal online behaviour that increases risk (e.g., sharing personal information, cyberbullying, illegal downloading).
 - Behaviour expectations online mirror our school behaviour policy.
 - Pupils are taught digital citizenship and respectful online communication.
4. **Commerce** – risks from online gambling, advertising, phishing, or financial exploitation.
 - Pupils are educated about in-app purchases, scams, and advertising.
 - Staff monitor and report any concerns about children being exploited financially online.

4.1 The 'Student Acceptable Use Policy' (Appendix 2) reminds pupils about their responsibilities and details the strategies to maximise learning opportunities whilst reducing potential risks associated with use of the internet.

5. Managing the ICT infrastructure

- 5.1 To effectively manage internet access (including all relevant security issues) the academy will:
- block all 'chat rooms' and social networking sites other than those which are part of a recognised educational network or approved learning platform
 - only unblock (on a strictly time-limited basis) other external social networking sites for specific purposes/internet literacy lessons
 - block access to music download or shopping sites other than those approved for recognised educational purposes at a regional or national level

- use security time-outs on internet access where practicable
- Inform all users that internet use is open to continuous monitoring
- make clear that in no circumstances is it acceptable for any individual to log on as another user
- set up the network with shared work areas for (separately) pupils and staff (pupils and staff are given appropriate instruction in how to save (and subsequently access) work to (or from) these areas)
- require all users to log off at all times when they have either finished working or are leaving the computer unattended (and in the event that a user finds a computer which is logged on but unattended they are required to always log off and then log on again as themselves).

In the interests of protecting themselves and others, pupils should be encouraged to bring such instances to the attention of a member of staff in order that suitable instruction may be offered to the previous user.

- set up the network so that users cannot download executable files/programmes
- make clear that the academy's IT department is responsible for ensuring that all equipment that is taken off site has full anti-virus and spyware protection and that this level of protection is maintained throughout in accordance with academy protocols and procedures
- make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the academy is used solely to support their professional responsibilities
- ensure that access to the academy's network resources from remote locations by staff is restricted to authorised personnel and that access is only through school approved systems
- ensure all staff and pupils have signed an acceptable use agreement form.
- Mobile devices may connect to the network but only when permitted and with full compliance with the ICT policies and Acceptable Use policy

6. ICT Security

- 6.1 All personal data held on ICT systems including USB sticks and other portable ICT equipment must be confidentially and permanently destroyed in line with the Records Management and Retention Policy prior to a device being destroyed.
- 6.2 If any ICT equipment is no longer in use by the school and is to be disposed of in any way, then the ICT Manager must ensure that all personal data has been removed from that system prior to its disposal.
- 6.3 If any ICT equipment is damaged and repairs are to be carried out by a third party then the equipment must be assessed to see what, if any, personal data is held on that equipment and any personal data should be protected before the equipment is provided to the third party for repair.
- 6.4 All users need to be aware that any ICT system device suspected of being infected with a virus must be disconnected from the network and reported to the ICT manager as soon as possible. The ICT manager must then take steps to remove the virus and protect the system.

7. Security Breaches

- 7.1 All suspected or actual breaches of ICT security shall be reported to the ICT Manager, the Headteacher and the Data Protection Officer in line with Section 3 above.
- 7.2 Steps must be taken by the ICT Manager or designated person, to ensure that the adequate protections are put in place as soon as a breach is suspected.
- 7.3 Steps must be taken to identify the cause of the breach and to update any policies and procedures to try and avoid the breach occurring in the future.
- 7.4 Any risk to personal data caused by the breach must be reported to the Data Protection Officer and the necessary steps under the Data Protection Policy for dealing with breaches should be followed.

8. School website

- 8.1 The headteacher has overall responsibility for ensuring that the website content is accurate and that the quality of presentation is maintained in full compliance with the statutory DfE guidelines for publications.
- 8.2 The content of the website will consist primarily of material created by the academy itself. Where the content has been published by others (or there are links to such material) the sources will be credited, with a clear statement as to the originator's identity or status.
- 8.3 Points of contact detailed on the website are likely to include the academy postal address, telephone number and certain email addresses (normally presented in a generic style such as 'info@schooladdress' or 'admin@schooladdress'). Personal information such as individual e-mail identities will not be disclosed.
- 8.4 Any photographs (whether of staff or pupils) published on the web will not have full names attached to them, and neither will names be recorded when saving images either in files or in tags when publishing photographs on the academy website.
- 8.5 Teachers using academy approved blogs (or similar) will be expected to ensure that these are password protected and to post contributions from the school website only.

9. Use of ICT equipment at home

- 9.1 In appropriate circumstances staff and pupils may be permitted to borrow academy ICT equipment for a time-limited period to pursue core school activities at home. Approval for requests must always be granted before equipment is removed from school premises and the staff member or student must agree and sign the 'Acceptable Use Agreement' (Appendices 3 and 4 respectively).
- 9.2 Staff should be aware that there are only a limited number of such devices and the academy is under no obligation to provide this equipment on demand. If the equipment/computer is used to connect with the internet from the staff member's home, the academy will not be responsible for any costs involved.

9.3 The academy may (as and when resources permit):

- provide a laptop (or other IT equipment) for staff use at home or outside of school
- ensure that the equipment is working and that repairs are dealt with as quickly and effectively as possible
- ensure that the computer is covered by insurance for use in and out of school for study purposes, providing reasonable care is taken to prevent loss or damage
- ensure that the computer is protected against computer viruses and malware
- maintain and update any software used in school.

10. Use of digital and video photographic images

10.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have either recorded themselves or have downloaded from the internet.

10.2 However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may potentially cause significant harm or embarrassment to individuals in the short or longer term.

10.3 When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. Pupils should, in particular, be made aware of the risks attached to publishing their own images on the internet, for instance on social networking sites.

10.4 Images taken and used by the academy will not be kept for longer than is necessary and will be subject to appropriate security measures.

10.5 Staff are permitted to take digital/video images to support educational aims, but must follow academy procedures concerning the sharing, distribution and publication of those images, namely that:

- such images should only be taken on school equipment (the personal equipment of staff should never be used for this purpose)
- care should be taken that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute

8.6 In relation to pupils:

- they must not take, use, share, publish or distribute images of others without their express consent
- photographs taken by pupils for official school use will be controlled by the academy
- photographs published on the website and other publications (such as newsletters etc) which include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- their full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission will be obtained from parents/carers (normally in the form of completion of the appropriate Acceptable Use Agreement) before photographs of pupils (or examples of their work) are published on the academy website, around school and in school publications.

11. CCTV and monitoring

- 11.1 The academy has CCTV on the premises as part of site surveillance for staff and student safety. Recordings will not be revealed without permission except where disclosed to the police as part of a criminal investigation.
- 11.2 Specialist lesson recording equipment may be used on occasion as a tool to share best teaching practice. These recordings are only accessible to authorised members of staff and will not be used for any other purposes.

Breaches of this policy

- 12.1 The ICT Manager, Head teacher and the DPO are responsible for reviewing and monitoring compliance with this policy in line with section 3 above.
- 12.2 Any reports of staff, governors or third parties breaching this policy should be reported to the Headteacher and investigated fully. Any breaches will be taken seriously.

13. Other policies and procedures

- a. This policy will be supported by the following policies and procedures:
- Behaviour Policy (student)
 - Code of Conduct and Practice
 - Disciplinary Policy
 - Safeguarding Policy
 - Social Media Policy

Appendix 1: Staff Acceptable Use Policy on E-safety

Principles

As an organisation with responsibility for safeguarding of pupils it is important that all staff take every possible necessary measure to protect data and information systems from unauthorised access, infection, damage, loss, abuse and theft.

All members of staff have a responsibility to use the school's information technology equipment in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and related school systems, they are asked to read and sign this Acceptable Use Policy.

Definitions

School Information and Communication Technology

This means any computer, networking device, telephone, copier, printer, fax machine, or other Information and Communication Technology equipment which

- is owned by the school or
- is licensed or leased by the school or
- is subject to school policies.

Roles and responsibilities

The school

The school owns the computers and the internal computer networks used on site. The school also has various rights to the software and information residing on, developed on, or licensed for these computers and networks. The school administers, protects, and monitors this aggregation of computers, software, and networks.

In its management of Information and Communication Technology, the school and its administrative department takes responsibility for:

- focusing central Information and Communication Technology resources on activities connected with teaching, learning and administration
- protecting school networks and other shared facilities from malicious or unauthorised use
- ensuring that central school computer systems do not lose important information because of hardware, software, or administrative failures or breakdowns
- managing computing resources so that members of the school community are not denied fair and equitable access to them
- establishing and supporting acceptable standards of security for electronic information that community members produce, use, or distribute, and ensuring the privacy and accuracy of all data processed by the school
- delineating the limits of privacy that can be expected in the use of networked computer resources and preserving freedom of expression over this medium without countenancing abusive or unlawful activities
- monitoring policies and communicating changes in policy as events or technology may warrant
- enforcing policies by restricting access and initiating disciplinary proceedings as appropriate.

The Individual

The school supports networked information resources to further its mission of teaching and learning. All members of the school community must be aware of the rules and conventions that make these resources secure and efficient. Users of school Information and Communication Technology will take responsibility for:

- using resources efficiently, and accepting limitations or restrictions on computing resources - such as storage space, time limits, or amount of resources consumed - when asked to do so by systems administrators
- ensuring that programs from the internet are not downloaded or installed on any school computer: advice should be sought from the ICT Manager as appropriate
- backing up files and other data regularly and permanently removing old files no longer required
- preventing unauthorised network access to or from their computers or computer accounts (this includes the responsible monitoring by staff of student users in their charge)
- recognising the limitations to privacy afforded by electronic services
- respecting the rights of others to be free from harassment or intimidation
- Only devices approved by the ICT Manager should be permitted to be connected to the network. The guest access or staff access network must be used for any visitor or personal devices.
- ensuring the physical protection of school Information and Communication Technology equipment (and understanding that any damage or theft is to be reported to the technical support staff immediately upon detection)
- ensuring responsible use of ICT equipment and ensuring pupils are following the Acceptable Use Policy
- reporting any faults, problems or requests to the ICT Support Team using the appropriate channels as soon as possible.

In addition the following “traffic light” system should help you make effective use of these technologies.

The Family of Learning Trust - ICT Traffic Light System

Red (Do not engage in these activities)

- Use your personal email address for work related business.
- Use e-mail to engage in gossip.
- Make libelous statements about individuals or other organisations.
- Make statements purporting to represent the Trust when they are personal views.
- Make derogatory remarks or express derogatory opinions about the Trust.
- Knowingly infringe copyright or intellectual property rights.
- Knowingly send or receive anything which is illegal or fraudulent.
- Knowingly send or receive material which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver (or anyone who sees the material) harassment, alarm or distress.
- Use the facility to pursue personal business interests, for gambling or for political purposes not directly related to your job.
- Allow anyone else to use your user name and password to gain internet access.
- Knowingly engage in any activity which threatens the integrity or availability of the Trust's systems.
- Attempt to break into (HACK) any area.
- Allow mobile phones to ring during working time.
- View/update or post on social media accounts during work time.

Amber (Seek your manager's approval prior to engaging in the activity)

- Opening and/or sending personal e-mails in working time.
- Personal browsing, purchases of goods and services via the internet in working time.
- Use mobile telephones to receive or make/send personal calls or text messages in work time.

Green (Legitimate use)

- Communicate by e-mail or mobile phone on behalf of the Trust or as an aid to pursuing tasks within the employee's job remit.
- Conducting research into work related matters.
- Personal research of the internet or sending personal e-mails outside working hours.
- Personal purchases of goods and services via the internet outside working hours.
- Opening personal e-mails outside working time.
- Receive/sending personal text messages outside working time.
- Receiving/making personal calls outside working time.
- View/update or post on school social media accounts as part of your designated role.

This list is neither exclusive nor exhaustive. If you are in any doubt about using ICT facilities for a particular purpose, please ask a member of the Senior Management Team. If you inadvertently access a site that contains illegal or offensive material, please inform a member of SLT or the ICT Manager immediately.

Any failure to comply with the acceptable use of Cyber Security and Social Media Policies may constitute gross misconduct and could lead to disciplinary action.

.....

I have read and understood and agree to comply with the Staff Acceptable Use Policy on Cyber security.

Signed:

Print Name:

Job Title:

Date:

Appendix 2: Student Acceptable Use Policy on E-safety

(Year 5/6 to complete at the discretion of the head teacher)

This Acceptable Use Policy is intended to ensure that young people will be responsible users while using the internet and other communications technologies for educational, personal and recreational use. The school will ensure that ICT systems and users are protected from accidental or deliberate misuse that could place the security of the systems and users at risk.

School strategy

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General

- Internet sessions will always be supervised by a staff member
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material
- The school will regularly monitor pupils' internet usage
- Pupils and teachers will be provided with training in the area of Internet safety
- Uploading and downloading of non-approved software will not be permitted
- Virus protection software will be used and updated on a regular basis
- The use of personal floppy disks, memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission
- Pupils will always treat others with respect and will not undertake any actions that may bring the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils will ensure that they log out of their computer equipment when leaving the IT room.

Email

- Pupils will use approved class email accounts under supervision by or permission from a teacher
- Pupils will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person (including cyberbullying)
- Pupils will not reveal their own or other people's personal details, such as email password, addresses or telephone numbers or pictures
- Pupils will never arrange a face-to-face meeting with someone they only know through emails or the internet
- Pupils will note that sending and receiving email attachments is subject to permission from their teacher

World wide web

- Pupils will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials
- Pupils will report accidental accessing of inappropriate materials in accordance with school procedures
- Pupils experiencing any issues related to viruses or anti-virus software should inform the ICT Technician without delay
- Pupils will use the internet for educational purposes only
- Pupils will not copy information into assignments without express acknowledgement of the source material (plagiarism and copyright infringement)
- Pupils will never disclose or publicise personal information
- Downloading by pupils of materials or images not relevant to their studies is in direct breach of the school's acceptable use policy
- Pupils will be aware that any usage, including distributing or receiving information whether school-related or personal, may be monitored for unusual activity, security and/or network management reasons

Internet chat

- Pupils will only have access to chat rooms, discussion forums, messaging or other electronic communication that have been accorded prior approval by the school
- Use of chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised
- Usernames will be used to avoid disclosure of identity
- Face-to-face meetings with individuals arranged via internet chat will be expressly forbidden.

Use of digital/video images

The use of digital/video images plays an increasingly important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of learning and activities. These images may then be used in presentations in subsequent lessons or to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

We will ensure that when such images are published pupils cannot be identified by the use of their names.

Internet use and access is considered a school resource and privilege which, if the school AUP is not adhered to, will be withdrawn and appropriate sanctions (as outlined in the AUP) imposed.

Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

School website

- Pupils will be given the opportunity to publish projects, artwork or schoolwork on the world wide web in accordance with clear policies and approval processes regarding the content that may be included in the school's website
- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff
- Website using facilities such as guest books, noticeboards or weblogs will be checked frequently to ensure that they do not contain personal details
- The publication of student work will be co-ordinated by a teacher
- Pupils' work will appear in an educational context on web pages with a copyright notice prohibiting the copying of such work without express written permission
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual pupils will not be published on the school website without parental permission. Video clips may be password protected
- Images will not be taken of any student against their wishes
- Photographs taken by our pupils will be controlled by the school and staff will ensure that they are appropriately supervised in line with the school e-safety policy
- Personal student information including home address and contact details will not be included in school web pages
- The school website will not publish the names of individuals in a photograph
- Pupils will continue to own the copyright on any work published.

Personal devices

Pupils are not allowed to use their own devices in school for personal use. This includes such use as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorised taking of images with a mobile phone camera. All of these activities will be deemed to be in direct breach of the school's acceptable use policy.

Legislation

The school will provide information on the following legislation relating to use of the internet (with which teachers, pupils and parents may care to familiarise themselves):

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- Data Protection Act 1988

Support structures

The school will inform pupils and parents of key support structures and organisations that deal with illegal material or harmful use of the internet.

Sanctions

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

Name of Student: _____ **Class/Year:** _____

Student

I have read and understood, and agree to follow, the school's Acceptable Use Policy on the use of the internet. I undertake to use the internet in a responsible way and to obey all the rules explained to me by the school.

Student's signature: _____

Name of student: _____

Date: _____

Parent/Guardian

Although the school takes active steps to promote safe use of the Internet, it recognises the possibility that pupils may accidentally or deliberately access inappropriate or objectionable material.

The school respects each family's right to decide whether or not to allow their children access to the Internet as defined by the school's Acceptable Use Policy.

I agree to the school taking and using digital/video images of my child/children. I also agree to other organisations such as the press or partner organisations associated with our school and other organisations visited by pupils (such as Alton Towers) taking and using digital/video images of my child/children that is compliant with the Data Protection Act. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access the internet. I understand that internet access is intended for educational purposes.

I also understand that every reasonable precaution has been taken by the school to provide for online safety but that the school cannot be held responsible if pupils access unsuitable websites.

I accept the above paragraphs ☐ **I do not accept the above paragraphs** ☐
(Please tick as appropriate)

In relation to the school website and other school material (such as newsletters) I accept that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the school website and other school material. I understand and accept the terms of the Acceptable Use Policy relating to publishing pupils' work on the school website or in school material/newsletters.

I accept the above paragraph ☐ **I do not accept the above paragraph** ☐
(Please tick as appropriate)

Parent's signature: _____

Date: _____

Parent/Carer name: _____

Appendix 3: E-safety Loan Agreement – Staff

Staff may borrow school Information and Technology laptop computers for a time-limited period to pursue core school activities at home. Approval for all requests must be authorised from a member of the senior leadership team prior to equipment being removed from school premises.

Staff are expected to:

- report promptly any loss or damage (including accidental loss or damage)
- report promptly to the IT department any faults in hardware or software
- ensure that the equipment is returned at the end of the agreed time or as soon as the employee ceases to be employed at our school or upon request (whichever is earlier)
- ensure that the equipment is not used for any illegal and/or anti-social purpose, including access to inappropriate internet sites and chat rooms
- ensure that programmes other than those provided by the school are not loaded without prior permission
- take reasonable precautions to prevent the introduction of viruses (and if in any doubt whether a virus may have contaminated the equipment this must be reported before the equipment is connected to the school network)
- ensure that the equipment is transported appropriately and kept securely and protected from damage
- refrain from creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place.

Failure either to take such reasonable care or to abide by the other conditions listed in this document may result in the computer/equipment being reclaimed. The school also reserves the right to claim financial recompense in such cases (in addition to which disciplinary action may be invoked).

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

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

Type of equipment: Laptop (brand) (serial number)

Camera Video camera Other (specify)

Member of staff signature:

Job Title:

Name

Date:

Authorised signatory (SLT)

Date:

Name:

Appendix 4: E-safety Loan Agreement – Pupils

In order to improve their learning experiences in and out of the classroom pupils may borrow school Information and Technology equipment including laptop computers for a time-limited period to pursue core school activities at home. Approval for all requests must be authorised by a member of the senior leadership team prior to equipment is being removed from school premises.

Pupils are expected to:

- report promptly any loss or damage (including accidental loss or damage)
- report promptly to the IT department any faults in hardware or software
- ensure that the equipment is returned at the end of the agreed time or as soon as the student ceases to be on roll at our school or upon request (whichever is earlier)
- ensure that the equipment is not used for any illegal and/or anti-social purpose, including access to inappropriate internet sites and chat rooms
- ensure that programmes other than those provided by the school are not loaded without prior permission
- take reasonable precautions to prevent the introduction of viruses (and if in any doubt whether a virus may have contaminated the equipment this must be reported before the equipment is connected to the school network)
- ensure that the equipment is transported appropriately and kept securely and protected from damage
- refrain from creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place.

Failure either to take such reasonable care or to abide by the other conditions listed in this document may result in the computer/equipment being reclaimed. The school also reserves the right to claim financial recompense in such cases (in addition to which disciplinary action may be invoked).

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

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

Type of equipment: Laptop (brand) (serial number)

Camera Video camera Other (specify)

Student signature:

Year group:

Name

Date:

Authorised signatory (SLT)

Date:

Name: