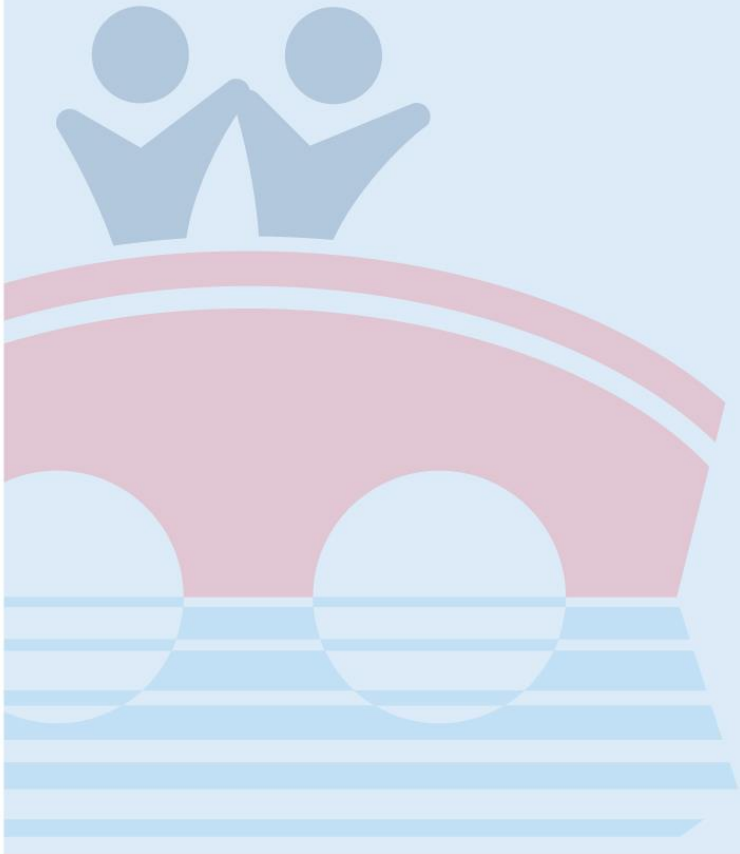
Altarnun
Primary School

Altarnun Primary E-Safety Use Policy



a member of
ALAT
www.alat.org.uk

Altarnun Primary School

Contents

1. Mission Statement

Adventure Learning Academy Trust (ALAT) AND Bright Tribe Trust (Bright Tribe) brings a new energy and approach to providing the best education for our students. Through proven practices, ALAT / Bright Tribe will transform the learning of students, raise standards and provide the highest quality learning environments, enabling students and teaching staff to thrive and be the best. ALAT / Bright Tribe's aim is to break down the barriers that limit educational progress. We do this through adopting a personal learning pathway for every child – one that takes account of individual needs, aspirations and talents.

ALAT / Bright Tribe's values:

Learn	Grow	Prosper
Provide the best education for every student.	Grow our students' futures.	Lead the way in education.
Ensure the highest quality teaching and learning.	Develop the best teaching staff.	Realise the opportunities.
Work with the family, parent or carer.	Provide the best learning environment and supporting technology.	Be connected to the community.

2. Introduction

ALAT / Bright Tribe acknowledges that ICT is an essential resource at the heart of teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. We understand that our academies need to embrace the use of these technologies in order to equip our young people with the skills to access life-long learning and employment.

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning and we recognise the constant and fast paced evolution of ICT within our society as a whole. We recognise that children and young people use a wide range of technologies both inside and outside of the classroom, and we believe that it is vital that they can continue to use these technologies safely and securely.

Similarly, we know that ICT is a vital component in the running and administration of any organisation, including our academies and ALAT / Bright Tribe itself. We identify the technologies that may be used in our organisation or an academy includes but is not limited to:

- Websites (secure and unsecure)
- E-mail, Instant Messaging and chat rooms
- Social media, including Facebook and Twitter
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web/internet functionality
- Gaming, especially online
- Learning platforms and virtual learning environments
- Blogs and Wikis

- Podcasting
- Video broadcasting
- Music downloading
- Media streaming (internet radio etc.)
- Secure remote access such as VPN or VNC
- VOIP telephony, video conferencing and other internet based communications technologies

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently monitored, or secure. All users need to be aware of the range of risks associated with the use of these technologies and that some have minimum age requirements, usually 13 years.

ALAT / Bright Tribe is committed to ensuring that its whole community is safe and secure, and takes its responsibility to educate its staff and students on e-safety issues very seriously. We will positively influence all of our community to be safe when using technology; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using ICT, in and beyond the context of the classroom.

As an academy trust we collectively hold personal data on students, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in adverse media coverage, and potentially damage the reputation of the school, as well as potentially result in a fine from the Information Commissioner. Everybody in our community has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

This Acceptable Use Agreement (for all staff, governors, visitors and students) covers the use of all types of ICT equipment, both fixed and mobile; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.) and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring

In order for ALAT / Bright Tribe to successfully implement our community approach to e-safety and Data Security, we feel that it is necessary for us to adopt a policy of monitoring. Whilst we respect the privacy of all members of our community, we also feel that it is very important that we are collectively empowered to prevent any incident where any member of our community may come to harm because of misuse of ICT equipment.

Authorised ICT staff may inspect any ICT equipment owned or leased by any member of the ALAT / Bright Tribe community at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification and contact the ALAT / Bright Tribe ICT director. Any ICT authorised staff member will be happy to comply with this request.

Authorised ICT staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving the employees or contractors of ALAT / Bright Tribe, or any of our member academies, without consent, to the extent permitted by law.

This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of ALAT / Bright Tribe's ICT; for quality control or training purposes; to comply with a subject access request under the Data Protection Act 1998, or to prevent or detect crime.

Authorised ICT staff may, without prior notice, access the e-mail or voice-mail account where applicable, of a member of staff who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by authorised ICT staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. Please note that personal communications using ALAT / Bright Tribe's ICT resources may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

ALAT / Bright Tribe takes any breaches of this Acceptable Use Policy very seriously, and where an incident is suspected, or reported will always take any necessary action to ensure the safety of all members of the community as a priority.

A breach or suspected breach of policy by any employee, contractor or guest may result in the temporary or permanent withdrawal of ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the ALAT / Bright Tribe disciplinary procedure. It should be noted that policy breaches might also lead to criminal or civil proceedings.

The ICO's new powers to issue monetary penalties came into force on 6th April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office (ICO) are to:

- Conduct assessments to check organisations are complying with the Act
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law
- Prosecute those who commit criminal offences under the Act
- Conduct audits to assess whether organisations processing of personal data follows good practice
- Report to Parliament on data protection issues of concern

Where necessary, ALAT / Bright Tribe will report incidents to the ICO and will fully comply with any recommendations or actions resulting from communications with the ICO.

Incident Reporting

ALAT / Bright Tribe wishes to ensure that all members of staff can report incidents of breaches of this policy and/or related incidents without fear of reprisals. As such, all reports will be dealt with in the strictest confidence.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Principal and/or e-safety co-ordinator. Additionally, all security breaches,

lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited e-mails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your line manager at your earliest convenience.

Core Acceptable Use Statements

ALAT / Bright Tribe's AUP is based on the following core statements, which we feel are fundamental in upholding our policies regarding e-safety and data protection.

All users must take responsibility for their own use of ICT equipment, making sure that they use technology safely, responsibly and legally in accordance with this policy

- All users must be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by all technologies, especially those accessed online
- No communications device, whether school provided or personally owned, may be used for the bullying, harassment, discrimination or abuse of others in any form
- No applications or services accessed by users may be used to bring ALAT / Bright Tribe, it's community, any member academy, or its staff, into disrepute
- No applications or services accessed by users may be used for any activity that may in any way be deemed to be illegal, offensive or dangerous. All ICT usage is subject to the provisions of the Computer Misuse Act 1990
- All users have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others in or connected to ALAT / Bright Tribe
- All users have a duty to respect the technical safeguards that are in place at ALAT / Bright Tribe – any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable
- All users have a duty to report failings in technical safeguards which may become apparent when using the systems and services
- All users have a duty to protect their passwords and personal network logins - and should log off or lock the device when leaving any ICT equipment unattended
- All users should make every effort to ensure that the data that they have access to is secure and safe at all times. Users should not move, transport, transmit or send any data without appropriate encryption, security and safety measures being used
- Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- All users should use network resources responsibly. Wasting staff effort or networked resources, or using the resources in such a way so as to diminish the service for other network users, is unacceptable
- All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- All users should be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures might come into action, including the power to check and/or confiscate personal technologies such as mobile phones.
- All users must take responsibility for reading, signing and upholding the standards laid out in the staff AUP

- All users should understand that the AUP is regularly reviewed and consistently enforced
- In order to ensure that all members of our community are able to fully comply with these core statements, we will at all times ensure that:
- All of the necessary documentation, guidelines, resources and policies are available for all staff to enable them to comply with this policy
- All of the necessary procedures, escalation routes and training are in place to allow all staff to complete their obligations within the policy

3. E-Safety

What is E-Safety?

The term 'e-safety' is used to encompass the safe use of all on-line technologies in order to protect pupils from potential and known risks.

Managing the use of on-line technology

E-Safety Lead

At Altarnun Primary School the E-Safety Lead is Katie Dalton, who is also one of the designated leads for safeguarding. The responsibilities of the lead person include:

- Updating the E-Safety and Acceptable Use Policy
- Ensuring that policies and procedures include aspects of E-Safety
- Work with the IT Technicians and ICT Coordinator to ensure that the filtering is set at the correct level for staff and children
- Ensure staff training is provided on E-Safety issues
- Ensure E-Safety is included in staff induction
- Monitor and evaluate incidents that occur to inform future safeguarding developments

Principles of the Teaching and Learning of E-Safety

The purpose of using on-line technology in school is to raise educational standards to promote pupil achievement and engagement, to support professional work of staff and to enhance the schools' management, information and business administration systems. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.

In addition to accessing the internet at school, we recognise that children will use the internet and other digital technology on their own time at other locations and are at greater risk if they have not been taught what the dangers are and how to use them safely. Supporting and assisting the development of children's e-confidence, and their ability to access the digital world effectively and safely is essential.

We acknowledge that the range of risks to young people in the digital environment is wide and ever changing e.g. 'Grooming' by sexual predators via internet-enabled multi-player games and social networking sites is not uncommon.

At Altarnun, we recognise the importance of raising the awareness in children so that they are able to keep themselves as safe as possible when using the internet and other digital technologies. In order to do this, we involve children and their parents/ carers in the safe use of on-line technologies.

Children are taught what on-line technology use is acceptable and what is not and given clear objectives for its use. Children are educated in the effective use of on-line technology in research, including skills of knowledge location, evaluation and retrieval. Lessons on E-Safety are also delivered as part of the ICT Curriculum.

We support the Youth Charter of Digital Rights because a key element of child protection in the digital environment is developing the skills and confidence of young people in the face of threats to their safety, enabling them to adopt the safest possible behaviour's themselves and to be able to report situations and behaviours of others that could constitute a threat. These messages are more likely to be adopted and taken to heart by children if presented in terms of their own rights than if presented as a set of rules about what they shouldn't do.

Comment [SJ1]: Is this the same in Cornwall?

We provide support and guidance to pupils and their parents/carers for the safe and responsible use of these on-line technologies. A partnership approach with parents is encouraged and guidance regarding e-safety is offered to parents in a variety of different ways e.g. information evenings, relevant links and documents on the school website and workshops.

School Website

Website photographs that include pupils will be selected carefully. Pupil's full names will not be used on the website in association with photographs unless written permission from parents/carers is obtained.

Chat and instant messaging

Staff and pupils will not be allowed access to public or unregulated chat rooms. Pupils will not access social networking sites at school e.g. 'My Space, Bebo and Facebook'.

Photographic, video and audio technology

It is not appropriate to use photographic or video devices in changing rooms or toilets. Care should be taken when capturing photographs and video to ensure that all pupils are appropriately dressed. Staff may use photographic or video devices (school equipment only) to support school trips and curriculum activities. Pupils should always seek permission of their teacher before making audio, photographic or video recordings within the school grounds. It is the class teacher's responsibility to find out and ensure that no child without permission to have their photograph/video taken is included in such activities.

Mobile Phones

Children must not bring mobile phones to school. Staff must have their mobile phones on silent during teaching times and they must be kept out of sight. The use of mobile phones to take pictures or videos is strictly forbidden.

Assessment of Risk

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure the users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not

possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the Trust can accept liability for the material accessed, or any consequences of internet access. The use of a computer system without permission of for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly. The Principal will ensure that the E-Safety and Acceptable Use Policy is implemented and compliance with the policy monitored.

Responses necessary when a risk to a child is discovered

Prompt action is required if a complaint is made regarding the use of on-line technology. The facts of the case must be established and presented to the e-safety lead. A minor transgression of the rules may be dealt with by the class teacher as part of normal classroom discipline. Other situations could be potentially more serious and a range of sanctions will be used in line with our Behaviour Policy. Concerns of a child protection nature will be dealt with in accordance with our Safeguarding Policy. Staff must alert the E-Safety/Safeguarding Lead as soon as possible and record the concern on a 'Safeguarding Incident Concern Record' form. Please refer to Appendix E- How to respond if a risk is discovered.

Any complaints about staff misuse of on-line technology must be referred to the Principal immediately.

Appendices

Appendix 1 - Staff ICT Acceptable Use Policy

Duty of Care

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from breaches of security, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the academy's computer system 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 the school systems, they are asked to read and sign this Acceptable Use Policy.

Acceptable Use Policy

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the academy & ALAT / Bright Tribe ethos, other appropriate policies and the Law.

- I understand that information systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, e-mail and social media sites**.**
- Academy owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password. (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word or my own name, and is only used on one system.)
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the systems manager.
- I will ensure that any personal data of students, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which may be removed from the academy site (such as via e-mail or on memory sticks or CDs) will be encrypted by a method approved by the academy, or in accordance with the academy data protection policy, which may forbid data from being taken off site at all. Any images or videos of students will only be used as stated in the school image use policy and will always take into account parental consent.
- I will not keep professional documents, which contain academy-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the Altarnun SharePoint to upload any work documents and files in a password-protected environment. I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the academy computer system that is unrelated to academy activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the ALAT / Bright Tribe e-safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the designated child protection coordinator **Katie Dalton** who is also the e-safety coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to **Jason Parks** the ICT Technician who is the designated lead for filtering as soon as possible.
- I will not attempt to bypass any filtering and/or security systems put in place by the academy. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any academy related documents or files, then I will report this to the ICT support provider/team.
- My electronic communications with students, parents/carers and other professionals will only take place via work approved communication channels e.g. via an academy provided e-mail address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the senior leadership team.
- My use of ICT and information systems will always be compatible with my professional role, whether using academy or personal systems. This includes the use of e-mail, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the academy AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the academy, or ALAT / Bright Tribe Trust, into disrepute.
- I will promote e-safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-safety coordinator, Katie Dalton.
- I understand that my use of the information systems, Internet and e-mail may be monitored and recorded to ensure policy compliance.
- ALAT / Bright Tribe and the academy may exercise its right to monitor the use of information systems, including internet access and the interception of e-mails in order to monitor compliance with this AUP and the academy's data security policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the academy will invoke its disciplinary procedure. If the academy suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the staff ICT Acceptable Use Policy

Name of Staff member: _____

Employment Number: _____

Signed: _____ Dated: _____

Appendix 2 – Student Acceptable Use Policy Agreement Template

Key Stage 1/ EYFS

Acceptable Usage Policy (AUP) KS1 Children – Linked to 360Safe AUP Guidelines

ICT equipment includes laptops, printers, scanners, cameras, data logging equipment, robots etc.

These rules have been written to make sure that you stay safe when using the computers and other ICT equipment. By using ICT in school, you have agreed to follow these rules. Your teacher will talk to you about these rules before you take them home to talk through with your parents. Your parent will then sign the form if they are happy that you have understood these rules.

If you have any questions, please ask your teacher.

The Golden Rule: **Think before you click**

- I will be careful when using or carrying equipment.
- I will only use the equipment I have been given for the task the teacher has set.
- I will follow instructions for using equipment carefully.
- I will remember to log off properly before closing the lid of the laptops.
- I will think before I print or delete.
- I will only use the internet when a teacher is with me.
- I will be sensible when going on the internet by only looking at pages that the teacher has asked me to use.
- I will tell a teacher if I see something that I don't like.
- I will keep my password secret, but I can tell my family.
- I will only logon using my username and password
- I won't put water bottles on the table when using ICT.

I have discussed these rules with my child and I am confident that my child understands them and the importance of keeping them.

Pupil Name: _____ Class: _____

Signed (Parent): _____ Date: _____

Key Stage 2

Acceptable Usage Policy (AUP) KS2 Children – Linked to 360Safe AUP Guidelines

ICT equipment includes laptops, printers, scanners, cameras, data logging equipment, robots etc.

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers, laptops and everything else including cameras and other devices. To use ICT in school, you need to agree to follow these rules. These rules will be discussed with you as a class before you take a copy home to discuss with your parents, sign and return to school.

If you have any questions, please ask your teacher.

- At all times, **I will think before I click** (especially when deleting or printing)
- When using the internet, I will only access websites related to the learning objectives of the lesson
- If I find a website or image that is inappropriate, I will tell my teacher straight away
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site
- When communicating online (in blogs, email etc.) I will think about the words that I use and will not use words that may offend other people
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number
- I understand that people online might not be who they say they are
- I will take care when using the computers and transporting equipment around
- I will not look at other people's files or documents without their permission
- I will not logon using another person's account without their permission
- I will think before deleting files
- I will think before I print
- I will save my work at regular intervals
- When I have finished using a computer, I will log off
- I know that the teachers can, and will, check the files and websites I have used
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers
- When using ICT, I will put water bottles in another place
- I will not use memory sticks without permission from the teacher
- I understand that if I am acting inappropriately then my parents will be informed

Signed (Pupil) _____ Class _____ Date _____

Appendix 3 – Youth Charter of Digital Rights

Youth Charter of Digital Rights

- You have the right to enjoy the internet and all the fun and safe things it has to offer.
- You have a right to keep information about you private. You only have to tell people what you really want them to know.
- You have a right to explore the internet but remember that you cannot trust everything that you see or read on the internet.
- You have a right to know who you are talking to on the internet; you don't have to talk to someone if you don't want to.
- Remember not everyone is who they say they are on the internet. You have a right to tell someone if you think anyone is suspicious.
- You have a right not to fill out forms or not to answer questions you find on the Internet.
- You have the right to **not** be videoed or photographed by anyone using cameras, web cams or mobile phones.
- You have a right not to have any videos or images of yourself put on the Internet, and you have the right to report it to an adult if anyone does this.
- You have a right **not** to be bullied by others on the Internet and you have the right to report this to an adult if this happens.
- If you accidentally see something you shouldn't you have the right to tell someone and not to feel guilty about it.
- We are **all** responsible for treating everyone on line with respect. You should not use behaviour or language that would be offensive or upsetting to somebody else.

Appendix 4 – Information and Websites

- **CEOP**

  http://www.ceop.gov.uk

- **Think U Know**

  http://www.thinkuknow.co.uk/Default.aspx?AspxAutoDetectCookieSupport=1

- **Childnet**

  http://www.childnet-int.org
  www.childnet.com/young-people
  www.childnet.com/resources/know-it-all-for-parents

- **Internet Watch Foundation**

  http://www.iwf.org.uk

- **BBC**

  www.bbc.co.uk/webwise/0/22728225

- **Child Line**

  www.childline.org.uk/explore/onlinesafety

- **Kid Smart**

  www.kidsmart.org.uk/parents

- **Safer Internet**

  www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls

- **Digital Unite**

  http://digitalunite.com/guides/internet-security/internet-safety-kids

Appendix 5 – How to respond if a risk is discovered

The E-safety lead will check that an adult follows these procedures in the event of any misuse of the Internet:

An inappropriate website is accessed inadvertently (ADULT):

- Report website to the E-Safety lead.
- Contact the IT Technician so that the site can be added to the banned or restricted list.
- Log the incident.

An inappropriate website is accessed inadvertently by a child or young person:

- Reassure the child/ young person
- Report website to the E-Safety lead.
- Contact the IT Technician so that the site can be added to the banned or restricted list.
- Log the incident.

An inappropriate website is accessed deliberately (ADULT):

- Ensure that no one else can access the material by shutting down the computer.
- Log the incident.
- Report to the Principal and E-Safety lead immediately.
- Principal to refer back to the Acceptable Use Policy and follow agreed actions for discipline (see discipline policy).
- Inform the IT Technician in order to reassess the filters.

An inappropriate website is accessed deliberately by a child or young person:

- Ensure that no one else can access the material by shutting down the computer.
- Log the incident.
- Inform E-Safety Lead
- Refer the child to the Acceptable Use Policy.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction.
- Notify the parent/carer.
- Contact the IT Technician to notify them of the website.

An adult receives inappropriate material:

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Principal immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police, social care
- Log the incident

An illegal website is accessed or illegal material is found on a computer. (The following incidents must be reported directly to the police):

- Indecent images of children found. (Images of children whether they are or cartoons of children or young people apparently under the age of 16, involved in sexual activity or posed in a sexually provocative manner)
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Criminally racist or anti-religious material
- Violent or bomb-making material
- Software piracy
- The promotion of illegal drug-taking
- Adult material that potentially breaches the obscene publications act in the UK.

If any of these are found, the following should occur:

- Alert the Principal and E-Safety lead immediately.
- DO NOT LOG OFF the computer but disconnect from the electricity supply.
- Contact the police and or CEOP and social care immediately

If a member of staff or volunteer is involved, refer to the allegations against staff in the Safeguarding Policy and report to the Local Authority Designated Officer.

An adult has communicated with a child or used ICT equipment inappropriately (e-mail/ text message etc.)

- Ensure the child is reassured and remove them from the situation.
- Report to the Principal and Designated Person for Child Protection immediately, who will then follow the Allegations Procedure and Child Protection Procedures as set out in the Safeguarding Policy
- Report to the Local Authority Designated Officer.
- Preserve the information received by the child if possible.

- Contact the police as necessary.

Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:

- Preserve any evidence and log the incident.
- Inform the Principal immediately and follow the Safeguarding Policy.
- Inform the E-Safety Lead so that new risks can be identified.
- Contact the police.

Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Principal.

Threatening or malicious comments are posted to the school website or learning platform about a child in school or malicious text messages are sent to another child/young person (cyber bullying).

- Preserve any evidence
- Log the incident.
- Inform the E-Safety Lead and Principal
- Contact parents/ carers.
- Refer to the Anti-Bullying Policy.
- Contact the police or CEOP as necessary

Appendix 6 – Legal Framework

This section is designed to inform users of legal issues relevant to the use of Communications. It is not professional advice.

The Sexual Offences Act 2003,

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an Offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images, such as videos, photos or web cams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with who they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape. More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent; there is no need to prove any intent or purpose.

Data Protection Act 1998

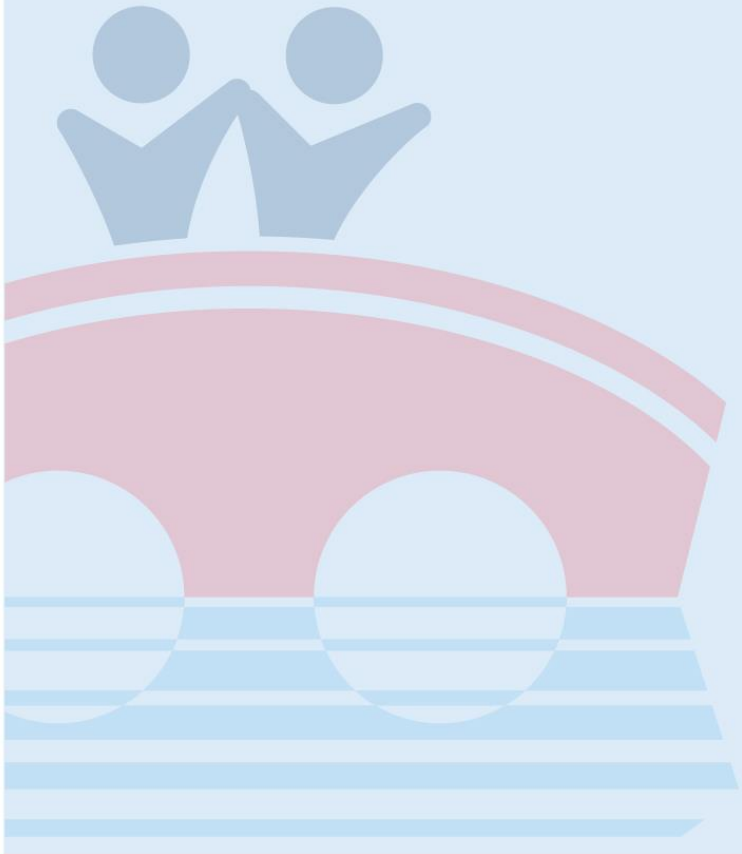
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to: gain access to computer files or software without permission (for example using someone else's password to access files); gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or impair the operation

Altarnun Primary School

Five Lanes Launceston Cornwall PL15 7RZ
Telephone 01566 86274 Email secretary@altarnunprimary.org.uk
www.altarnunprimary.org.uk



a member of
ALAT
www.alat.org.uk