

## Curzon CE Combined School

### ICT E-Safety and Acceptable Use Policy (AUP) for staff and pupils

#### OBJECTIVES

- ensure pupils' internet use and access is appropriate and controlled.
- prevent misuse of internet connected devices.
- ensure pupils and parents/carers are educated on the risks carried with internet use and how to minimise and deal with those risks.
- provide students with knowledge and resources to make decisions to ensure their safety online
- ensure that staff use ICT responsibly.
- ensure procedures and access for staff and pupils are effectively managed to minimise risks
- enable our pupils to grow into respectful and safe global citizens
- teach the importance of respecting others online – this fit with our Curzon value of courage.

The school has provided PCs and electronic devices as an important tool for teaching, learning, and administration of the school. Use of these by both members of staff and pupils, is governed at all times by the following policy. Any questions or concerns should be directed to the ICT Network Manager in the first instance. This policy should be read in conjunction with other policies, eg. Anti-bullying, Behaviour, Complaints, Child Protection, Disciplinary, Extremism and Radicalisation, ICT, GDPR and codes of conduct.

All members of the school community have a responsibility to use the school's computer system in a professional, lawful, and ethical manner, for their own protection and the school's. Use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. However, deliberate abuse of the school's computer system may result in disciplinary action (including possible termination of contract), and civil and/or criminal liability. This policy is not intended to arbitrarily limit the ways in which staff can use the system, but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation of the school, and to ensure the safety of all users. All school systems are also to ensure all users of the school network are not only protected with regards to GDPR but also in accordance with the statutory PREVENT guidance published by the Government. The filtering system will help to ensure that content related to radicalisation and extremism is blocked.

The school recognises that the distinction between computer use at work and at home is increasingly blurred, with many staff now using their own electronic devices for work. While the school neither wishes nor intends to dictate how staff use their own computer, laptop or phone, staff should consider that the spirit of this policy applies whenever they are undertaking an activity that stems from their employment with the school.

The Education and Inspections Act 2006 empowers Headteachers to regulate the behaviour of pupils when they are off the school site as far as is reasonable and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. It is impossible to eliminate all risks completely so it is essential to build pupils' awareness and resilience to the risks to which they may be exposed, teach them to be responsible users and be safe while using the internet and other communication technologies. This is also pertinent to cyber-bullying and other e-safety incidents which may take place out of school but are linked to its membership and can affect the school ethos. The school wishes to ensure that all adults within the school community present positive role models to the children in their dealings with the school and with one another, seeking to foster the school's Christian distinctiveness at all times. The school will, where known, inform and

## ***'Learning, sharing and growing under God.'***

express concern to any who show inappropriate e-safety behaviour and inform parents / carers of incidents of inappropriate pupil e-safety behaviour that take place both inside and outside of school.

### **RELEVANT LEGISLATION**

It is recommended that legal advice is sought from officers in ODBST in the advent of an e safety issue or situation.

Computer Misuse Act 1990	Protection of Children Act 1978
Data Protection Act 1998	Sexual Offences Act 2003
Freedom of Information Act 2000	Public Order Act 1986
Communications Act 2003	Obscene Publications Act 1959 and 1964
Malicious Communications Act 1988	Human Rights Act 1998
Regulation of Investigatory Powers Act 2000	The Education and Inspections Act 2006
Trade Marks Act 1994.	The Education and Inspections Act 2011
Copyright, Designs and Patents Act 1988	The Protection of Freedoms Act 2012
Telecommunications Act 1984	The School Information Regulations 2012
Criminal Justice & Public Order Act 1994	Serious Crime Act 2015
Racial and Religious Hatred Act 2006	Keeping Children safe in Education 2022
Protection from Harassment Act 1997	

### **KEY AREAS**

#### **Curriculum**

E-safety is a focus in all areas of the curriculum and all staff reinforce e-safety messages across the curriculum.

The school has a planned e-safety curriculum as part of Computing/ICT, PHSE and other lessons which is regularly revisited

Key e-safety messages are reinforced as part of a planned programme of assemblies, events and tutorial and pastoral activities

Pupils are taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information

Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Pupils are taught to respect copyright when using material accessed on the internet

Pupils are helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

Staff act as good role models in their use of digital technologies, the internet and mobile devices

## ***'Learning, sharing and growing under God.'***

Pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.

Staff are vigilant in monitoring the content of the websites the young people visit.

Where pupils research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

### **Computer Security and Data Protection**

- Staff are provided with a personal account for accessing the school computer system, with their own username and password. This account will be tailored to the level of access they require and is for their use only.
- Staff **must not allow a pupil to have individual use of a staff account** for any length of time, even if supervised.
- When leaving a computer unattended, staff **must** ensure they have either logged off their account or locked the computer to prevent anyone using their account in their absence.
- To support GDPR compliance, staff **must** not save school data on any other devices than the Staff Portal or One Drive including when working from home.
- Staff **must** ensure that items of portable computer equipment (such as iPads, laptops) are not left unattended when the school has multiple visitors on site such as an Open Morning or after school parents' meetings.
- Equipment taken offsite is not routinely insured by the school. If staff take any school equipment offsite, they should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft.
- When using social media, those within the school community should never share work log-in details, passwords, personal phone numbers, email addresses whether their own or those of pupils or parents. Staff should restrict access to social media sites and pages and where possible, not add parents to their access list and vice versa.
- Those working with children have a duty of care and should maintain appropriate boundaries so that information cannot be misused by third parties for "cyberbullying" or identity theft or be perceived as grooming. New employees should check any information they have placed on social media sites and remove anything that might cause embarrassment or offence immediately they start at the school.
- Staff should not use their personal phones to contact pupils or parents, nor take photographs on their phones but seek permission from a member of the senior management team where this might be deemed necessary. When calling from home if school is closed, staff must block their numbers using 141 and record conversations. If speaking to pupils, they should ask for the pupil to be put on speakerphone at home.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that it must be for limited purposes, relevant, accurate and secure.
- Staff must ensure that personal data is kept secure and used only on secure password protected school devices. Memory sticks are not permitted due to being high risk of being lost or misplaced with the contents then being open to misuse.
- Curzon has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it. This records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). The school will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. (The Trust's 'retention policy' applies to the deletion and disposal of data supports this). All staff receive GDPR annual training.

### **Use of Social Networking websites and online forums**

## ***'Learning, sharing and growing under God.'***

Staff must take care when using social networking websites such as Facebook or Instagram, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave them open to misinterpretation or abuse, increasing the likelihood that the school's reputation could be impacted. The sites also rarely make little or no distinction between adult users and children. As part of the recruitment process, school will check the person's social media profile.

Staff must not allow any pupil to access personal information they post on a social networking site. In particular:

- Staff **must** ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
- Staff **must not** add a pupil to their 'friends list'. They may have their parents' permission, but many social media websites require users to be aged 13 or over. Pupils may request after leaving the school, but a friendship link is not recommended before they reach the age of 18.
- Staff should avoid contacting any pupil privately via a social networking website, even for school-related purposes.
- Staff should take steps to ensure that any person contacting them via a social networking website is who they claim to be, before allowing them access to any personal information.
- Staff should be aware that their reputation can be harmed by what others share and say about them, such as friends tagging them in inappropriate posts, photographs or videos.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, staff **must not** post content on websites that may appear as if they are speaking for / representing the school.
- Staff should not post any material online that can be clearly linked to the school and could damage the school's reputation.
- Staff should avoid posting any material which clearly identifies themselves, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

It is a good idea for staff to keep a check on their online presence eg by typing their name into a search engine to check. If there is negative content online connected to a member of staff, it is better to deal with this as soon as is possible with knowledge / support from a manager. Screen prints of any messages or abuse should be taken with the time and date.

The school seeks to foster a positive image and reputation and it is important to understand that light hearted or unguarded comments can cause untold damage to individuals and the establishment which can take much time and effort to undo. If there is a pressing need to leave comments that could be associated with the school, they should be qualified with a clear statement that "the opinions expressed here do not necessarily reflect those of my employer" and the name of the school and colleagues should be omitted.

Where an aggressive or abusive perpetrator is a local person, leaders or governors should contact the person to raise their concerns and request that the person removes the offending detail immediately. If the person refuses, the matter can be reported to the website, support sought from The UK Safer Internet Centre (The Professional Online Safety Helpline) or to the LA/ODBST Legal team. If the comments are threatening or abusive, the Police should also be contacted.

The school's filtering system does not allow pupils access to social media sites.

### **Use of Email**

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the school. The following considerations must be made when communicating by email:

### ***'Learning, sharing and growing under God.'***

- E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. Staff **must** be cautious when sending both internal and external mails. Ensure the spell checking facility is switched on. The professional standards that apply to internal memos and external letters must be observed for e-mail.
- E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, and where appropriate, obtain legal advice before sending. Staff **must not** purchase goods or services on behalf of the school via e-mail without appropriate authorisation.
- **All school e-mails sent should have a footer containing name, job title and the name of the school.**
- E-mail is not a secure method of communication, and can be easily copied, altered, forwarded and archived. Unless explicitly authorised to do so, staff **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the school.
- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The school will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users.
- Staff must not send chain letters or unsolicited commercial e-mail (also known as SPAM).
- During school closure, staff will use the 'Homework' email only to communicate with parents, not their personal work emails.

Pupils at Curzon do not have email accounts.

#### **Use of digital and video images - Photographic, Video**

Staff, pupils, parents and governors need to be aware of the risks associated with sharing images and posting them on the internet as they may remain available forever and may cause harm or embarrassment to individuals. School employers may carry out internet searches for information about potential and existing employees. The school will inform and educate users about the risks of potential for harm when using digital images. In particular:

- there is a need for pupils to recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- pupils must not take, use, share, publish or distribute images of others without their permission.
- staff are allowed to take digital / video images to support educational aims but must follow school policies for sharing, distributing, and publishing those images. Staff will aim to use school equipment to take the images.
- photographs published on the website or elsewhere that include pupils, will be selected carefully and will comply with good practice on their use.
- pupils are to be appropriately dressed, positioned and not participating in activities that might bring them or the school into disrepute.
- pupils' full names will not be used without full agreement of parents.
- written permission from parents or carers will be obtained when the child starts school and annually before photographs or digital images are used. Staff will check the school's master permissions list before using images on the web.

Video calling during School Closure times - The school may use either Microsoft teams or Zoom for small groups of children/classes. Virtual meetings may also be held with parents.

- The parent or carer must make sure their child and other members of the household are aware the video call is happening. The parent should stay in the room.
- Where possible, 2 members of school staff will be on each call.



### ***'Learning, sharing and growing under God.'***

- Children or parents should not take screen shots of the call.
- For GDPR reasons, children should use only first names on a call. When meeting with parents remotely, we will ask them to use surnames only e.g. Mr Jones.
- Staff, children and other members of the household must wear suitable clothing
- Devices used should be in appropriate areas, for example, not in bedrooms; and where possible against a neutral background. Children may be asked to switch on video cameras for safeguarding purposes
- Language must be professional and appropriate, including any family members in the background.
- The same expectations apply for remote teaching and conversations as normal school conduct
- Staff will only ever video call a pupil with prior agreement with parents and the head teacher or deputy. This will always be at a pre-arranged time with a password sent via email. The times of all video calls and lessons will be logged.
- Parents will need to appear on screen at the start of the lesson to confirm they give consent for their child to be part of the group conversation.
- Wherever possible 'live' classes will be recorded so that if any issues were to arise, the video can be reviewed. Parents and children will be asked to confirm they are aware of this and give consent at the start of each session.
- The waiting room function will be used and private messaging dysfunctional.

#### **Supervision of Pupil Internet Use**

- Pupils **must** be supervised by a teacher or adult at all times when using school computer equipment to access the Internet.
- Supervising staff are responsible for ensuring that the separate pupils' ICT code of conduct is enforced (**Appendix 6**).
- Supervising staff **must** ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.
- In lessons where internet use is pre-planned, pupils are guided to sites which staff have checked to be suitable beforehand and that processes are in place for dealing with any unsuitable material that is found in internet searches (i.e. first response is for pupil to switch off screen and quietly inform a member of staff).
- Staff should teach pupils to understand, follow e safety rules. Pupils should be regularly reminded of the need for e-safety. Teaching will include how they should deal with any unsuitable material found in searches. Staff should teach pupils the importance of adopting good e-safety practice out of school too.

#### **Privacy**

- **Staff are not permitted to access social media websites or pursue outside interests from the school's computers or other devices at any time unless authorised to do so by a member of the senior management team. Abuse of this is generally considered to interfere with levels of productivity and will be considered a disciplinary matter.**
- Use of the school computer system, including their email account and storage areas provided for their use, may be subject to monitoring by the school/ IT Network Manager to ensure compliance with this AUP and applicable laws. This may include remote monitoring of an interactive logon session. The school has access to a record of sites visited on the Internet by both pupils and staff.
- Staff must not store sensitive\*(Note 1 at end of policy) personal information on the school computer system that is unrelated to school activities (such as personal passwords, photographs, or financial information).

## ***'Learning, sharing and growing under God.'***

- The school may use measures to audit use of computer systems for performance and diagnostic purposes.
- **Use of the school computer system indicates staff's consent to the above described monitoring taking place.**

### **Confidentiality and Copyright**

- Respect the work and ownership rights of people outside the school, as well as other staff or pupils.
- Staff are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material they wish to use, download or copy. Even if materials on the school computer system or the Internet are not marked with the copyright symbol (©), staff should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
- Staff **must** consult the IT Network Manager before placing any order of computer hardware or software, or obtaining and using any software they believe to be free. This is to check that the intended use by the school is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the school's systems.
- As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by them during the course of their employment in any way affecting or relating to the business of the School or capable of being used or adapted for use within the School, shall be immediately disclosed to the School and shall to the extent permitted by law, belong to and be the absolute property of the School.

### **Reporting Problems with the Computer System**

It is the job of the IT Network Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

- Staff should report any problems that need attention to the IT Network Manager as soon as possible. Problems that seriously hinder their job or teaching and require immediate attention should be reported by email or if serious, by telephone.
- If staff suspect their computer has been affected by a virus or other malware, they **must** report this to the IT Network Manager **immediately**.
- If staff have lost documents or files, they should report this as soon as possible. The longer a data loss problem goes unreported, the less the chances of the data being recoverable (mere minutes can count).

### **Reporting Breaches of this Policy**

All members of staff have a duty to ensure this AUP is followed. Staff **must** immediately inform the IT Network Manager or the Headteacher of abuse of any part of the computer system. In particular, staff should report:

- any websites accessible from within school that they feel are unsuitable for staff or pupils
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by themselves, another member of staff, or a pupil via the school computer system.

Written reports should be made and given to both the Headteacher and IT Network Manager. Reports concerning breaches of information should be made to the Data Protection Officer at the ODBST. All reports will be treated confidentially.

## **Technical – infrastructure equipment, filtering and monitoring**

Curzon has a managed IT service provided by TIO with an IT Network Manager assigned to our school. ODBST is clear that it is the responsibility of the LGB to ensure that the managed service provider carries out all the E-safety measures that would otherwise be the responsibility of the school. It is also important that the managed service provider is fully aware of the trust's and school's E-safety Policy and the agreed Acceptable Use Agreements.

It is the devolved responsibility for LGBs to ensure that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved are implemented. It will also need to ensure that the relevant people are effective in carrying out their E-safety responsibilities

A more detailed Technical Security Policy Guidance can be sourced from the trust, however, Trustees are clear that in ODBST schools:

- School / Academy technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password
- A named individual is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users and content lists are regularly updated and internet use is logged and regularly monitored by TIO.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet
- There is a clear process in place to deal with requests for filtering changes (see ODBST School Technical Security Policy Guidance for more details)
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages and different groups of users – staff, pupils, parents etc.) .

Personal data cannot be sent over the internet or taken off the ODBST site unless safely encrypted or otherwise secured

## **Personal Use**

The school recognises that occasional personal use of the school's computers is beneficial both to the development of their IT skills and for maintaining a positive work-life balance. Such use is permitted at the discretion of the school, but can be revoked at any time and is subject to the conditions that it:

- **must** comply with all other conditions of this AUP as they apply to non-personal use, and all other school policies regarding for e.g. staff conduct;
- **must not** interfere in any way with their other duties or those of any other member of staff;
- **must not** have any undue effect on the performance of the computer system; and
- **must not** be for any commercial purpose or gain unless explicitly authorised by the school.

## **Use of staff's own equipment**

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and **must not** be



## ***'Learning, sharing and growing under God.'***

used until approved. This test must be performed at regular intervals as required by the school's procedures on electrical safety testing.

- Staff **must not** connect personal computer equipment to school computer equipment without prior approval from the ICT Network manager.
- When working from home on personal devices, staff must ensure they do not save documents to their hard drives and instead to the Share point.

### **CONDUCT**

- Staff **must** at all times conduct their computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:
  - The school's social media policy applies to all who work on the school site, including volunteers and community users where their work brings them into contact with the pupils. This applies to any social media that they use, both at work and in their personal lives and should be read in conjunction with this policy.
  - Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, extremist, racist, sexist, or defamatory language or materials;
  - Making ethnic, sexual-preference, or gender-related slurs or jokes.
- Staff **must** respect, and not attempt to bypass, security or access restrictions in place on the school computer system.
- Staff **must** not intentionally damage, disable, or otherwise harm the operation of school computers.
- Staff **must** make efforts not to intentionally waste resources. Examples of resource wastage include:
  - Excessive downloading of material from the Internet;
  - Excessive downloading of large numbers of photographs
  - Excessive storage of unnecessary files on the network storage areas;
  - Use of printers to produce class sets of materials, instead of the photocopier.
  - Multiple use of colour copies
- Staff should avoid eating or drinking around computer equipment to reduce likelihood of spillage damaging equipment.
- All use of the Internet is subject to filtering and monitoring undertaken the school in order to satisfy current safeguarding requirements and to ensure online safety for all.

**Pupil Conduct- see appendix 6.**

**Unsuitable / inappropriate activities** Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images –The making, production or distribution of indecent images of children.
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986
- Pornography
- Promotion of any kind of discrimination
- Threatening behaviour, including promotion of physical violence or mental harm

## ***'Learning, sharing and growing under God.'***

- Promotion of extremism or terrorism
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Such action could lead to criminal prosecution.

### **Activities that might be classed as cyber-crime under the Computer Misuse Act:**

- Gaining unauthorised access to school networks, data and files, through the use of computers/device
- Creating or propagating computer viruses or other harmful files
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Disable/Impair/Disrupt network functionality through the use of computers/devices
- Using penetration testing equipment (without relevant permission)

**Trustees believe that the activities referred to below, would be inappropriate in a school context or, in some cases risk disclosing personal passwords and bank details on open school systems and that users should not engage in these activities when using school equipment:**

### **Using school systems to run a private business**

- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy
- Infringing copyright
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- On-line gambling
- Use of messaging apps

### **Responding to incidents of misuse**

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

#### **Illegal Incidents**

- If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to DSL and ODBST and report immediately to the police.

#### **Other Incidents**

ODBST expects all members of the school community to be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, ODBST expects its senior leaders and governors to act promptly and to take all the steps in this procedure:

### ***'Learning, sharing and growing under God.'***

- Have more than one senior member of staff and/or governor involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the investigation using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- Ensure during the investigation that the sites and content visited are closely monitored and recorded (to provide further protection); recording the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the record (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated, the individual will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement ODBST officers or national/local organisations (as relevant).
  - Police involvement and/or action

**If the content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- offences under the Computer Misuse Act (see Appendix G)
- other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the investigating panel for evidence and reference purposes.

It is more likely that our schools will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that pupils are aware of the standards in place to minimise any breaches. It is expected that incidents of misuse will be dealt with through normal behaviour policies and procedures as follows. Each incident will be treated case by case. The table below gives an indication of the types of responses and sanctions which may be given.

***'Learning, sharing and growing under God.'***

Students/Pupils Incidents	Refer to class teacher	Refer to Headteacher	Refer to MAT	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/exclusion
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).</b>		X	X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons		X			X	X	X	X	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X				X	X	X	
Unauthorised/inappropriate use of social media/ messaging apps/personal email		X			X	X	X	X	
Unauthorised downloading or uploading of files	X	x	X		X			X	
Allowing others to access school/academy network by sharing username and passwords	X	x	X		X			X	
Attempting to access or accessing the school/academy network, using another student's/pupil's account	X	x	x		X			X	
Attempting to access or accessing the school/academy network, using the account of a member of staff	X	x	x		X	X	x	X	x
Corrupting or destroying the data of other users	X	x	X		X	X	X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	x	X			X	x	X	
Continued infringements of the above, following previous warnings or sanctions		x	X			X			X
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school		X	X		x	X	x	X	X
Using proxy sites or other means to subvert the school's/academy's filtering system		x	X		x	X	x	X	X

***'Learning, sharing and growing under God.'***

Accidentally accessing offensive or pornographic material and failing to report the incident		X			x	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material		x	x	x	x	X	x	X	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		x	x		x				

	Actions/Sanctions							
	Refer to line manager	Refer to Headteacher Principal	Refer MAT/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Staff Incidents								
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).</b>		X	X	X	X		X	X
Inappropriate personal use of the internet/social media/personal email		x	x			X	X	X
Unauthorised downloading or uploading of files		X	x		x	x		



***'Learning, sharing and growing under God.'***

Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		x	x		x	x	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner		x			X	X		
Deliberate actions to breach data protection or network security rules		x	x		x	x	x	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x		x	x	x	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x			x	x	X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		x	x	x	x	x	x	X
Actions which could compromise the staff member's professional standing		x	x			x	x	X
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy		x	x		x	x	x	X
Using proxy sites or other means to subvert the school's/academy's filtering system		x	x		x	x	x	X
Accidentally accessing offensive or pornographic material and failing to report the incident		x	x		X	X		
Deliberately accessing or trying to access offensive or pornographic material		x	x	x	x		X	X
Breaching copyright or licensing regulations		X	x		x	x		
Continued infringements of the above, following previous warnings or sanctions		x	x	X	x		x	X

## **ROLES AND RESPONSIBILITIES**

### **The role and responsibilities of the IT Network Manager:**

The IT Network Manager is responsible for ensuring that:

- monitoring and filtering systems are installed, updated and effective.
- the school's IT infrastructure is secure and not open to misuse or malicious attack.
- the school meets the recommended technical requirements.
- the school's networks are password protected.
- he/she keeps up to date with e-safety technical information, actions and brings information and updates to the school

## ***'Learning, sharing and growing under God.'***

- the network is monitored regularly to identify misuse/attempted misuse. Any incidents are reported to the Headteacher for investigation and action.
- Only the IT Network Manager will have password admin access

### **The Headteacher will ensure that:**

- all staff receive suitable training and updates to enable them to carry out their e-safety roles well, ensuring uniform and consistent practice and to be equipped to train other colleagues / pupils.
- that all staff are aware of the procedures to be followed in the event of an e-safety incident.

**Local Governors: have devolved responsibility for the approval of their E-safety Policy and for reviewing the effectiveness of their policies.**

### **E-safety Coordinators (head teacher)**

- take day to day responsibility for e-safety issues and a leading role in establishing and reviewing the school e-safety policies
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provide training and advice for staff
- liaise with external bodies
- report on e-safety incidents to the Senior Leadership Team and keep a log of incidents to inform future e-safety developments
- meet with the governors to discuss current issues, review incident logs and filtering / change control log

### **Teaching and Support Staff**

- have an up to date awareness of e-safety matters and of the current school AUP and practices
- have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- report any suspected misuse or problem to the Headteacher investigation & action
- all digital communications with pupils and parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- ensure that pupils understand and follow the e-safety and acceptable use policies
- monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

### **Pupils**

Pupils have a role to play in ensuring that their learning is supported by the safe, respectful and secure use of the internet, new technologies and mobile devices. to remain both safe and legal when using the internet, they will need to understand the appropriate behaviours and critical thinking skills and show they:

- are responsible for using the school digital technology systems in accordance with the school's Acceptable Use Policy
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- know and understand policies on the use of mobile devices and digital cameras.
- know and understand policies on the taking/use of images and on cyber-bullying at an age-appropriate level.

## ***'Learning, sharing and growing under God.'***

- understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's AUP covers their actions out of school, if related to their membership of the school

### **Parents / Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Parents are informed about e safety through e safety meetings, curriculum meetings and newsletter updates and high profile events, such as e safety day and anti-bullying week.

ODBST would expect parents and carers to be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to on-line student / pupil records

### **Community / Other Users**

Community and other users who access our schools' systems will be expected to sign a Community User Acceptable Use Agreement (AUA) before being provided with access to school systems. (A Community Users AUA for PTA can be found in the appendices.)

### **Review and Evaluation**

The Curriculum Committee is responsible for this policy and for reviewing and monitoring its effectiveness.

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

### **Notes**

1. "Sensitive personal information" is defined as information about an individual that is protected by law under the Data Protection Act 1998. Examples of such data include addresses and contact details of individuals, dates of birth, and pupil SEN data. This list is not exhaustive. Further information can be found in the school's GDPR Policy.

I have read this policy and agree to abide by it.

Name .....

Signed .....

Date .....

September 2022

## APPENDIX 1

### **Staff Internet Code of Practice**

#### **Staff (and Volunteer) Acceptable Use Policy Agreement**

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 when at school and at home.
- 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, chrome books, email, Pupil/Staff Portal 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 primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- 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 ICT 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 / Curzon Pupil site /Pupil

### ***'Learning, sharing and growing under God.'***

Portal) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.
- 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 on-line activity that may compromise my professional responsibilities.

The school and the Trust 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 (laptops / iPads / mobile phones / chrome books etc) 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 which may be set by the ODBST and 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.
- I will ensure that my data is regularly backed up, in accordance with school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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 and prevent other users from being able to carry out 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, unless this is allowed in school policies.
- 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 policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that General Data Protection Regulations require 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 loss of such data and 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 the 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



***'Learning, sharing and growing under God.'***

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 Policy Agreement, I could be subject to disciplinary action as set down in Trust HR policies 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.

I have read the Code of Practice for pupils and teachers and I am familiar with the school's policy on the use of the Internet, e-mail, the creation of web sites and network security.

I agree to abide by these policies and the Teachers' and Support Staff's Code of Practice.

Name .....

Signature.....

## **APPENDIX 2**

### **General Class iPad Agreement for all School Staff who use them**

Curzon CE School is committed to improving the access to learning and the personal development opportunities of its pupils. We believe the use of the Apple iPad in teaching and learning can help towards these goals and iPads are available to staff for this reason.

**Please sign below to agree to the following terms of use:**

1. These iPads remain the property of Curzon School and are for use by you, support staff and pupils. They must not be loaned to anyone other than staff for overnight or longer term use.
2. These iPads are electronically linked to school systems. Pupil iPads can be used without a password. They may be used to store appropriate picture and video images of pupils along with other personal information. This means that you must fully comply with high standards of data protection.
3. You are responsible for looking after these iPads. If left unattended, they must be placed in a secure place. The whereabouts of iPads should not be divulged to parents or other visitors to the school, outside of the school staff/governor team.
4. Loss or damage of a device should be reported to the school's Network Manager immediately.
5. Staff and pupil use of email and internet activity on i-pads will be monitored by the Network Manager in the same way that the school PCs are.
6. iPads are expensive and fragile items and their use must be supervised at all times. iPads should only be used when the teacher believes that all pupils present are capable of using them sensibly.
7. These iPads are configured with certain restrictions in place for your safety. You must not try to make changes to these settings.
8. Use of the iPad must adhere to all other school policies. Failure to do so may lead to disciplinary action. These iPads will be checked regularly for safety and for compliance with school policies. Outcomes will be reported to the Headteacher.

**I have read this agreement and fully understand that I need to adhere to all elements.**

**Staff member's name:** .....

**Signature:** ..... **Date:** .....

**INDIVIDUALLY ALLOCATED Staff iPad Further Agreement**

Curzon CE Combined School provides some individual Apple iPads for staff to enable them to carry out their role more effectively.

Please sign below to accept this iPad and agree to the following terms of use:

1. This iPad remains the property of Curzon School and is loaned to you for use within your job role. You may take the staff password protected iPad off-site if you plan to use it in a way that will benefit the school. Should you leave it unattended and it is stolen, you will be held responsible for its replacement. Should anyone else use it at home/off site, you are held responsible that their use is that which would be permitted by the school.
2. The iPad must remain in your possession and should be securely stored when not in use. Staff iPads must only be accessed by a password.
3. The iPad is connected to your school email account so might have access to personal information of pupils. The iPad might also be used to store personal information such as appropriate picture and video images of pupils. This means you must fully comply with the usual high standards of data protection.
4. This iPad is configured with certain restrictions in place. You must not try to make changes to the device that are passcode protected.
5. Any internet connection or downloading cost incurred outside of school or without permission, will be the responsibility of the member of staff who has been given the i-Pad and not be chargeable to the school.
9. This iPad is an expensive and fragile item and should be treated as such. It may be used in the classroom for teaching but any direct use by a pupil should only take place under direct supervision by you. Remember that personal information might be accessible on the device and you must fully comply with high standards of data protection.
6. If you leave the employment of the school the iPad must be returned in good condition to the Network Manager in good time before your official leaving date.

iPad Model: ..... Serial No.: .....

Staff member's name: .....

I have read this agreement and fully understand that I need to adhere to all elements.

Received by Signature: ..... Date: .....

## APPENDIX 3

### Summary of Types of Communication

The following table shows what may and may not be used at school:

	STAFF				OTHER ADULTS			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school but kept out of sight of pupils and parents and kept on silent	X				X			
Use of mobile phones in lessons or in playground				X				X
Use of mobile phones in social time	X				X			
Mobile phones should be taken on educational visits by staff so they can contact the office and the other leader in an emergency	X							
Taking photos of children on personal devices				X		X		
Use of school electronic devices	X					X		
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails		X						X
Use of chat rooms				X				X
Use of instant messaging				X				X
Use of social networking sites				X				X
Use of blogs outside of the School's blogs				X				X

Pupils are not permitted to bring mobile phones into school. Should it be necessary for before and after school contact, this should be discussed with the Office Manager and the phone kept in the office.

## APPENDIX 4

### Summary of Unsuitable / Inappropriate Activities

The school policy restricts internet usage as follows:

User actions		Allowed at certain times	Allowed with staff permission	Not allowed
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Sexually explicit images			X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation			X
	adult material that potentially breaches the Obscene Publications Act in the UK			X
	Any material deemed to be racist, discriminatory, pornographic or religious hatred			X
	threatening behaviour, including promotion of physical violence or mental/emotional abuse or harm			X
	any other information which may be offensive to colleagues, breaches the integrity of the ethos of the school or brings the school into disrepute			X
Using school systems to run a private business				X
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by BucksGfL and / or the school				X
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X
Creating or propagating computer viruses or other harmful files				X
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet			X	
On-line gaming (educational)		X		
On-line gaming (non educational)			X	
On-line gambling				X
On-line shopping / commerce			X	
File sharing			X	
Use of social networking sites				X
Use of video broadcasting eg Youtube			X	












## **APPENDIX 5**

### **AIDE MEMOIRE SUMMARY OF GUIDELINES ON E-SAFETY FOR ALL WITHIN THE SCHOOL COMMUNITY**

- These notes summarise the school's policy which can be obtained on request from the school office.
- Staff, pupils, parents and all who work with or have connections with the school are expected to be aware of the risks associated with access to inappropriate material.
- Constant vigilance is required to protect pupils from the effects of media misuse both at school and at home. This applies as much to downloading of software and games as to e-mail traffic.
- The school has controls in place and staff will guide pupils to suitable sites and monitor use. Parents are strongly advised to implement controls at home to develop consistency between school and home use.
- Care should be taken when using social media, as incautious, unguarded, derogatory and offensive remarks can cause serious harm which may be difficult to undo. The school will respond seriously to any remarks which are deemed to bring the school into disrepute or perceived to be in danger of damaging the school's reputation. A useful rule is that anything you would not say to someone's face is best left unwritten. Facebook users must be at least 13 years old.
- Pupils should be made aware of the risks associated with use of chat rooms as so called friends may not be what they seem.
- Instances of cyber bullying will be taken very seriously whether by text, e-mail or image. Anyone initiating or distributing such material can expect to face investigation and sanctions may result.
- Pupils and parents should not exchange e-mail addresses or private 'phone numbers with staff and should not engage in direct personal contact with staff by 'phone, text or e-mail but only through the school office.
- Pupils and parents should not become "friends" (nor be asked to) with members of staff as this could be considered as potential "grooming".
- Parents should be aware of the school policy on photographic images of pupils which may not be taken without the individual's permission. The school will always seek this from parents in the case of images used by staff for publicity and other official purposes. Pupils likewise will be taught to always seek an individual's permission before using any images.
- Parents, guardians and carers will be expected to sign a copy of the Pupils' Internet Code of Practice and support the school's policies on use of the internet before joining the school.
- Memory sticks are not to be used in school.
- Internet on the school premises should be for school use only.

(Appendix 6)  
**KS1 Acceptable Use Agreement**

*These rules will keep me safe and help me to be fair to others:*

<b>C</b>	<b>Communicate</b> 	The messages I send or information I upload will always be polite and sensible in line with our school values.
<b>O</b>	<b>Ownership</b> 	I will keep my logins and passwords secret from my friends and strangers.
<b>M</b>	<b>Meet</b> 	I will never arrange to meet someone I have only ever met on the Internet.
<b>P</b>	<b>Permission</b> 	I will not look at or change other people's files without their permission. I only click on links and buttons when I know what they do
<b>U</b>	<b>Use</b> 	I will only use the school's computers for schoolwork. I am aware that the school can check my internet use. I will not use a teacher's iPad or computer.
<b>T</b>	<b>Trust</b> 	I will only e-mail people I know or a responsible adult has approved. I will not open an attachment or download a file unless I know and trust the person who has sent it.
<b>I</b>	<b>Initiative</b> 	If I see anything I am unhappy with or I receive a message I do not like, I will not reply to it but I will show a responsible adult.
<b>N</b>	<b>Never</b> 	I will not attempt to visit Internet sites that I know to be banned by the school. I will not use the Internet unless an adult is with me and I will tell them which sites I am using.
<b>G</b>	<b>Goal</b> 	I understand that I must use school ICT systems in a responsible and kind way.

*I have read and understood these rules and agree to them.*








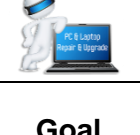

*Signed:*

*Date:*

**(Appendix 6b)**

**KS2 Acceptable Use Agreement**

*These rules will keep me safe and help me to be fair to others:*

<b>C</b>	<b>Communicate</b> 	The messages I send or information I upload at home or school will always be polite and sensible in line with our school values. I understand that all messages I send reflect on me and the school. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
<b>O</b>	<b>Ownership</b> 	I will not share my logins, IDs and passwords with friends and use the Pupil Portal responsibly. I will not give my personal information that could be used to identify me, my family or my friends on any online space at home or school, unless a trusted adult has given permission or reviewed the site first.
<b>M</b>	<b>Meet</b> 	I will never arrange to meet someone I have only ever known on the Internet, by email or in a chat room. I will talk to a trusted adult if someone asks me to meet them. I will use the Internet responsibly and will not visit websites that my parents or staff at school feel are inappropriate for school or my age.
<b>P</b>	<b>Permission</b> 	I will only edit or delete my own files and not view or change other people's files or user areas without their permission. I will be careful when opening files and attachments by checking for viruses etc. If I am unsure I will never open a file but seek guidance from an adult first. I will always ask permission before taking or uploading photos or information about others e.g. Do people mind you using their name in things?
<b>U</b>	<b>Use</b> 	I will only use the school's computers and iPads for appropriate school activities and learning and am aware that the school monitor my internet use. I am aware that some websites, games and social networks have age restrictions and I should respect this at school and at home.
<b>T</b>	<b>Trust</b> 	I will only e-mail or message people I know or a responsible adult has approved. I will not open an attachment or download a file unless I know and trust the person who has sent it. I will only comment if given permission at school and my comments will be respectful e.g. on Scratch
<b>I</b>	<b>Initiative</b> 	If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult. I will think critically about content I see online and apps I use; including whether they are to be trusted, whether I have checked terms and conditions of sites and apps, why they are free, and what information I am sharing to unknown others etc.
<b>N</b>	<b>Never</b> 	I will not bring files or USBs into school that can harm the school network or be used to interfere with school security tools. I will not share any personal data (my own or others) with anyone outside the school.
<b>G</b>	<b>Goal</b> 	I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of other users and the ICT systems. I will use my school account for educational and authorised purposes only, even at home.

*I have read and understood these rules and agree to them.*

*Signed:*

*Date:*

## **APPENDIX 7**

### **PTA ICT Code of Conduct**

**The members of the PTA committee have adopted the following principles:**

#### **General**

- We wish to fulfil all that is expected of a good volunteer, recognising that we have a duty to act fairly, responsibly and without prejudice.
- We will consider carefully how our decisions may affect staff, pupils and other parents, recognising the importance of a close and successful relationship with the school at all times. We will follow good e-safety guidelines, blind copying our communications to protect against misuse.

#### **Conduct**

We wish to work as a member of a team at all times and in so doing, be loyal to collective decisions. In our meetings and work together, we will:

- always be mindful of our responsibility to maintain and develop the ethos and reputation of our school
- seek to develop effective working relationships with the Headteacher, staff, parents and pupils,
- encourage expression of views at meetings, but maintain a level of professionalism at all times.
- accept collective responsibility for all decisions made by the PTA, not speaking out against majority decisions in public or private outside the PTA.
- only seek to act on behalf of the PTA or teacher when authorised to do so.
- follow planning documentation and risk assessments when making visits to school
- follow our children's and the school's code (respect and courtesy), when making or responding to any negative comments about the school.

#### **Communication**

As PTA committee members we wish to

- Promote close co-operation and communication, fostering good working relationships between parents, teachers, and the local community at all times.
- Recognise the valuable position they hold, in modelling school approach and level of commitment to other parents and if needed in bringing worries that parents might speak to them about to the attention of the school.
- Operate a duty of mutual trust and confidence to our school, and to each other, realising that this may be breached if unsuitable material is contained in any communication or correspondence, including all types of electronic communication, personal blogs, websites and social networking sites.
- Gain the agreement of the Chairman/Headteacher prior to posting any content (written, vocal or visual) to the internet which identifies us as members of the PTA

#### **Commitment**

We accept that being a member of the PTA committee involves commitment, time and energy. We wish to:

- be active and involved members, attend regularly, and share responsibilities,
- respond to opportunities to involve ourselves in school activities
- get to know and understand how the school prefers to function and
- prepare for meetings by reading paperwork beforehand

#### **Confidentiality**

***'Learning, sharing and growing under God.'***

We recognise the need to be discrete at times, especially regarding matters of data protection, individual staff or pupils and we will:

- not divulge information about members of staff or pupils inappropriately.
- exercise great care if a discussion of a potentially contentious issue of the school arises
- declare an interest if an item under discussion at any committee meeting impinges upon our personal, family or financial situation

SIGNED: .....

photocopied on to reverse)

(Appendix 5 School Aide Memoire



***'Learning, sharing and growing under God.'***

**1 Responding to incidents of misuse – record form**

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

**1.3.1.1 Details of first reviewing person**

Name: .....

Position: .....

Signature: .....

**1.3.1.2 Details of second reviewing person**

Name: .....

Position: .....

Signature: .....

**1.3.2 Name and location of computer used for review (for web sites)**

.....

.....

**1.3.2.1 Web site(s) address / 1.3.2.2 Reason for concern**  
**device**


1.3.2.3 D a t e	1.3.2.4 T i m e	1.3.2.5 Inci den t	1.3.2.6 Action Taken		1.3.2.7 Incid ent Rep orte d By	1.3.2.8 Sign atur e
			1.3.2.9 W ha t?	1.3.2.10 By Wh om ?		

1.3.2.11 Conclusion and Action proposed or taken
