Alkrington Primary School

Acceptable Use, E-Safety and Data Policy

RATIONALE

Computer technology in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

PURPOSE

At Alkrington Primary School we understand the responsibility to educate our children on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, 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 media coverage, and potentially damage the reputation of our schools. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school 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.

Both this policy and the Acceptable Use Agreement (at the end of this document) for all staff, governors, visitors and children, are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, etc); and technologies owned by children and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, tablets and portable media players, etc).

BROAD GUIDELINES

1. Monitoring

Authorised ICT staff (Simple IT), Headteacher, Deputy Headteacher or Computing Lead may inspect any ICT equipment owned or leased by the School 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 confirm their eligibility with the Headteacher.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, 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 School ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Register 2018 (GDPR), or to prevent or detect crime.

Web filtering software is used to filter, firewall and block /identify any inappropriate usage or unacceptable content. It also provides senior leadership with a monitoring report and urgent alerts where necessary.

ICT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone 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 ICT authorised staff and comply with the General Data Protection Register 2018 (GDPR), 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 school ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

2. Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the Local Authority Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

3. Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher. Additionally, all security breaches, lost/stolen equipment or data (including USB flash pens), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher with immediate effect (within 24 hours).

4. Computer Viruses

All files downloaded from the Internet, received via email or on removable media (CD, USB stick) must be checked for any viruses using school provided anti-virus software before using them. Never interfere with any anti-virus software installed on school ICT equipment that you use. If your machine is not routinely connected to the school network, you must make provision for regular virus updates through the ICT Technician. If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

5. Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. The expectations of staff are fully outlined in the school's Data Protection and Privacy Policy.

6. Security

The School gives relevant staff access to its Management Information System, with a unique ID and password. It is the responsibility of everyone to keep passwords secure. Staff are aware of their responsibility when accessing school data and they have been issued with the relevant guidance documents.

Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight. Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.

It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents copied, scanned or printed. This is particularly important when shared copiers (multifunction print, scan and copiers) are used. Anyone expecting a confidential/sensitive print or copy should have warned the sender to notify before it is sent.

7. Data Protection Officer (DPO)

The DPO is a senior member of staff (or contractor) who is familiar with information risks and the school's response. The DPO in this school is provided by Global Policing https://globalpolicing.co.uk/contact/

The role of the DPO is to understand:

- *what information is held, and for what purposes*
- *what information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff etc including UPN, teacher DCSF number etc)*
- *how information will be amended or added to over time*
- *who has access to the data and why*
- *how information is retained and disposed of*

As a result, the DPO is able to manage and address risks to the information and make sure that information handling complies with legal requirements laid down in the GDPR (2018). Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

8. Disposal of Redundant ICT Equipment Procedure

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed, or if the storage media has failed, it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

9. *Disposal of any ICT equipment will conform to:*

- *The Waste Electrical and Electronic Equipment Regulations 2006*
- *The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007*
  http://www.environmentagency.gov.uk/business/topics/waste/32084.aspx
  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
  http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
- *General Data Protection Register 1998 http://www.ico.gov.uk*
- *Electricity at Work Regulations 1989 http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm*

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal. The school's disposal record will comply with the Rochdale guidance and be within the delegated limits as defined by the school's Governors.

Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Further information is available at:

- *Waste Electrical and Electronic Equipment (WEEE) Regulations Environment Agency web site Introduction*
  http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
- *The Waste Electrical and Electronic Equipment Regulations 2006*
  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

- *The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007* *http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e* • *Information Commissioner website* *http://www.ico.gov.uk/*

11. **Email**

The use of email within school is an essential means of communication for both staff and children. In the context of school, email should not be considered private.

Pupils: We recognise that children need to understand how to style an email in relation to their age and use good network etiquette, or 'netiquette'. In order to achieve the KS2 computing expectations, children must have experienced sending and receiving emails. Children may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes. All pupil email users are expected to adhere to the generally accepted rules of netiquette, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, arrange to meet anyone without specific permission, or open attachments without virus checking them first. Children must immediately tell a teacher/trusted adult if they receive an offensive email. Children are introduced to email as part of the Computing Scheme of Work.

Adults: School provides staff with their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails, and avoids the risk of personal profile information being revealed. It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced.

The sending of emails is subject to the following:

- *The school email account should be the account that is used for all school business. Under no circumstances should staff contact children, parents, clients or conduct any school business using personal email addresses*
- *Language must not include swear words or be offensive or abusive*
- *Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted*
- *Sending of attachments which contain copyright material to which the school does not have distribution rights is not permitted*
- *The forwarding of any chain messages/emails etc. is not permitted*
- *Spam or junk mail will be blocked and reported to the email provider*
- *Attachments from an untrusted source should not be opened*
- *Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email*
- *Emails should never contain children's full names in the subject line. Initials or first names should be used wherever possible within the main body of the text*
- *Access to school email systems will always take place in accordance with data protection legislation and in-line with other appropriate school/setting policies e.g. confidentiality*
- *Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records*
- *Staff will be encouraged to develop an appropriate work life balance when responding to emails*
- *Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.*
- *School email addresses and other official contact details will not be used for setting up personal social media accounts.*
- *Emails created or received as part of the school email system will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000*

12. **Equal Opportunities**

Children with Additional Needs: School endeavours to create a consistent message with parents for all children and this in turn should aid establishment and future development of the school's E-Safety rules. However, staff are aware that some children may require additional teaching including reminders, prompts and further explanation to reinforce their existing

knowledge and understanding of E-Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

13. E-Safety

Roles and Responsibilities: As E-Safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety lead in this school is Greta McDonald, with this role overseen by the school safeguarding team. All members of the school community have been made aware of who holds this post. It is the role of the E-Safety Leader to keep abreast of current issues and guidance through organisations such as Rochdale LA, CEOP (Child Exploitation and Online Protection) and Childnet. Senior Leaders and Governors are updated by the Headteacher and E-Safety Leader and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

E-Safety in the Curriculum: ICT and online resources are used widely across the curriculum. We believe it is essential for E-Safety guidance to be given to the children on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- *The school has a framework for teaching internet skills in ICT lessons.*
- *The school provides opportunities within a range of curriculum areas to teach about E-Safety and during themed events, such as the annual Be Healthy, Be Safe Week.*
- *Educating children on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.*
- *Children are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.*
- *Children are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.*
- *Children are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Children are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.*
- *Children are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum.*

E-Safety Skills Development for Staff: Our staff receive regular information and training on E-Safety issues in the form of online references, INSET or staff meetings. New staff receive information on the school's acceptable use policy as part of their induction. All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community. All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

Managing the School E-Safety Messages: We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used. The E-Safety policy and practice is an integral part of everyday practice.

Misuse and Infringements: Complaints and/or issues relating to E-Safety should be made to the E-Safety Lead and Headteacher. Incidents should be logged and where necessary/appropriate referred to the relevant agency in accordance with personnel or safeguarding procedures.

Inappropriate Material: All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher and E-Safety Lead. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headteacher, depending on the seriousness of the offence; investigation by the Headteacher and Local Authority, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences. Users are made aware of sanctions relating to the misuse or misconduct as defined in the Staff Handbook and Guidance for Safer Working Practice for Adults Who Work With Children.

Internet Access: The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of it is logged. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet: Children have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.

- *Staff will preview any recommended sites before use*
- *Raw image searches are discouraged when working with children*
- *If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.*

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources. All users must observe copyright of materials from electronic resources. Temporary users will also need to comply with this policy

14. **Internet Use**

School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; General Data Protection Register (2018), The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.

Children and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If children wish to bring in work on removable media it must be checked using the school's anti-virus software before being opened.

Staff should seek to avoid the use of portable, removeable data devices e.g. USB stick, portable hard drive. They should instead seek to use online cloud-based services. However, if it is essential that staff use removable media, it is protected via the use of a password/encrypted device.

Internet Access

The Internet will be used in a variety of ways:

- to give access to a wide variety of education resources
- to exchange curriculum and administrative data
- to provide a source for research

Internet access for pupils will only take place when a member of staff is present. It is envisaged that children will have access to sites carefully selected by members of staff.

The school provides internet access for all staff and pupils in order to allow access to the wide range of content available. The school's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case, the website must be reported immediately to the E-Safety lead (Computing Co-ordinator). All members of staff need to understand that that they cannot rely on filtering alone to safeguard children. Supervision, classroom management and education about safe and responsible use is essential.

The use of the Internet is subject to the following:

- Supervision of pupils will be appropriate to their age and ability
- At Early Years Foundation Stage and Key Stage 1, pupils' access to the Internet will be by adult demonstration or directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability
- At Key Stage 1 and Key Stage 2, pupils will sign on the school network as themselves and be supervised. Pupils will use age-appropriate search engines and online tools. Online activities will be teacher-directed where necessary
- Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability
- It is not permitted to attempt to access, on any device, pornographic, illegal, sexist, violent, racist, gambling or inappropriate material in school

- The use of live chat rooms is not permitted.
- Members of the ICT Support Team have access to an unfiltered internet connection. Access is still only permitted to appropriate websites, unless directly instructed by the Headteacher for safeguarding training
- No member of staff may download any software from the internet for installation onto a school computer system without first consulting with a member of the ICT Support Team or Headteacher
- Staff must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Staff must not reveal names of colleagues, customers or clients or any other confidential information acquired through their job on any social networking site or blog

15. **Parental Involvement**

We believe that it is essential for parents/carers to be fully involved with promoting E-Safety both in and outside of school, and also to be aware of their responsibilities. We regularly consult and discuss E-Safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

Parents/carers and children are actively encouraged to contribute to adjustments or reviews of the school E-Safety policy. Parents/carers are asked to read through and sign acceptable use statement on behalf of their child on admission to school. Parents/carers are required to decide as to whether they consent to images of their child being taken/used in the public domain (e.g. on the school website, Twitter/X, newsletter etc.).

The school disseminates information to parents relating to E-Safety in a variety of ways, ranging from newsletters, social media and specific parental events.

16. **Passwords and Password Security**

Password Security: Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The children are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and children are regularly reminded of the need for password security. All users read and sign to demonstrate that they have understood the school's E-Safety Policy and Data Security.

Users are provided with an individual network, email, management Information System (where appropriate) log-in username.

Children are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others. Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and MIS systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Zombie Accounts: This refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- *Ensure that all user accounts are disabled once the member of the school has left*
- *Prompt action on disabling accounts will prevent unauthorised access*
- *Regularly change generic passwords to avoid unauthorised access (Microsoft advise every 42 days)*

17. **Personal or Sensitive Information**

Protecting Personal, Sensitive, Confidential and Classified Information

- *Ensure that any School information accessed from your own PC or removable media equipment is kept secure*
- *Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access*
- *Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others*
- *Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person*

- *Ensure the security of any personal, sensitive, confidential and classified information contained in documents you copy, scan or print. This is particularly important when shared multi-function print, scan and copiers are used and when access is from a non-school environment*
- *You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience*
- *Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information*
- *Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling*

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media
Where possible, we advise against the use of portable devices, instead recommending the use of online cloud services. But, where they are to be used, you must ensure removable media is purchased with encryption and that it is stored securely. Removable media that may hold personal data is securely disposed of. All files containing personal, sensitive, confidential or classified data is encrypted. Hard drives from machines no longer in service are removed and stored securely or wiped clean,

18. Remote Access

You are responsible for all activity via your remote access facility. Only use equipment with an appropriate level of security for remote access. To prevent unauthorised access to school systems, keep all access information such as logon IDs and passwords confidential and do not disclose them to anyone. Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

19. School ICT Equipment

As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you. Equipment issued to staff is logged and serial numbers are recorded as part of the school's inventory. Staff are to ensure that all ICT equipment that they use is kept physically secure. They are not to attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990. Staff are advised to save their data frequently. They are responsible for the backup and restoration of any of their data that is not held on the school's network drive. Personal or sensitive data should not be stored on the local drives of desktop PCs; if it is necessary to do so the local drive must be encrypted. We recommended that all staff have a time locking screensaver applied to their machines or PCs etc accessing personal data must have a locking screensaver as must any user profiles.
On termination of employment, resignation or transfer, staff are to return all ICT equipment to the school. It is the staff member's responsibility to ensure that any information accessed from their own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

20. Portable & Mobile ICT Equipment

This section covers such items as laptops, tablets and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

All activities carried out on school systems and hardware will be monitored as per the general policy. Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey. Portable and mobile ICT equipment has to be made available as necessary for anti-virus updates and software installations, patches or upgrades. The installation of any applications or software packages must be authorised by the ICT support team and be fully licensed. In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight. Portable equipment must be transported in its protective case if supplied.

21. Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, tablets, gaming devices, mobile and smartphones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use.

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

The use of the mobile devices by staff is subject to the following:

- *The school allows staff to bring in personal mobile phones and devices for their own use*
- *The school is not responsible for the loss, damage or theft of any personal mobile device*
- *The sending of inappropriate messages between any member of the school community is not allowed*
- *The school does not allow a member of staff to contact a pupil or parent/carer using their personal accounts However, staff can use their personal device to access approved methods for communication, such as Class Dojo and the school email system, providing this device is securely protected with a pin/password*
- *Staff must not use their mobile phone during lessons or other times when children are present*
- *Staff are not to leave lessons to take personal calls or messages, unless they have sought prior permission from a member of the senior leadership team where missing the call/message would have a significant detrimental impact, for example confirmation of a doctor's appointment*
- *Staff must not use their personal mobile device to take photographs or videos of pupils. Instead, staff are provided with a school tablet for this purpose. In EYFS, staff have been provided with smartphone - without a SIM card - instead of a tablet*

The use of the mobile devices by children is subject to the following:

- *Only children in Years 5 and 6 are allowed to bring their mobile phone into school. This is related to the safety of the child when travelling to/from school*
- *Devices are to be placed in a box at the start of the day, which is kept in the teacher's stockroom/cupboard until the end of the day*
- *The school is not responsible for the loss, damage or theft of any personal mobile device*
- *No devices are to remain in children's possession throughout the day, including in bags or coat pockets. Should children be identified as being in possession of their device, the device will be confiscated and secured safely by the teacher until the end of the day*
- *Where a child deliberately maintains possession of their device, at the discretion of the Headteacher the child may be banned from bringing their device into school and parents will be informed*

Removable Media: If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 'Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media'.

- *Only use recommended removable media*
- *Store all removable media securely*
- *Removable media must be disposed of securely by your ICT support team*

Servers: Servers holding personal data should be encrypted, therefore password protecting data. Servers are in a locked and secure environment and have limited access rights. Servers are password protected when locking the server. Servers have security software installed appropriate to the machine's specification and all data is backed up regularly. Back up media stored off-site must be secure and remote back-ups should be automatically securely encrypted.

Systems and Access: Staff are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC. They are not to allow any unauthorised person to use school ICT facilities and services that have been provided to them. They are only to use their own personal logins, account IDs and passwords and not to allow them to be used by anyone else. Staff are to keep their screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential or classified information. Staff are to ensure they have locked their screen before moving away from their computer during their normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.

Do Not Introduce or Propagate Viruses: Staff are not to access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone based on their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

Any information held on School systems, hardware or used concerning school-business may be subject to The Freedom of Information Act.

Any hard drives which may have held personal or confidential data must be 'scrubbed' in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whomever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple overwriting the data.

Telephone Services: You may make or receive personal telephone calls provided:

- *They are infrequent, kept as brief as possible and do not annoy others*
- *They are not for profit or to premium rate services*
- *They conform to this and other relevant school policies.*

School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused. Permission to make personal calls via the school telephone must be sought first. Staff are to be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

Staff are not to take personal incoming telephone calls via their own device during directed worktime unless prior permission has been sought.

Follow the appropriate procedures in the event of receiving a telephone call containing any information related to what could be classed as a Critical Incident. These procedures should be made readily available throughout your office. If you do not have a copy, please ask your line manager.

CONCLUSION

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and children, is to protect the interests and safety of the whole school community. There will be an on-going opportunity for staff to discuss with the E-Safety Lead or Senior Leaders any issue of E-Safety that concerns them. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way. It will be reviewed annually as part of the school safeguarding review procedures and consideration will be given to the implications for future whole school development planning.

Policy reviewed January 2024

Linked Policies

Data Protection and Privacy Policy
Safeguarding
Health & Safety
Behaviour
Anti-bullying
Home-School Agreement

Alkrington Primary School

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Executive Headteacher.

As a school user of the network resources / equipment I agree to follow the school rules (set out above) on its use. I will use the network/ equipment in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the E-Safety lead.

- I agree to report any misuse of the network to the E-Safety leader
- I agree to report any websites that are available on the school Internet that contain inappropriate material to the E-Safety leader
- I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the E-Safety leader or Head teacher

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signed _____ Date_____

Print name_____