HIGHFIELD ELY ACADEMY
An Active Learning Trust School

ACCEPTABLE USE of ICT and E-SAFETY POLICY
Inc: LINC 19-25 Provision

Ratified on: 28 June 2018

Review Date: June 2019

Introduction

This document is an addendum to the school's general ICT Policy. It addresses issues related to the acceptable use of the ICT facilities provided for children/adult learners, staff, parents, occasional community users and governors. Specifically it deals with the use of the school curriculum network, the Intranet that runs on this network, the publicly available school website and the facility for access to the Internet provided through the network. It has been produced in accordance with National Association of Advisers for Computers in Education (NAACE) guidelines.

Acceptable use of these facilities implies use which:

- Safeguards individuals from offensive messages, personal or impersonal, in any medium capable of being held on a computer system, e.g. malicious emails messages, pornographic images, etc.
- Safeguards the anonymity of individuals (particularly pupils/adult learners) and their computer-based work, when that is appropriate.
- Safeguards the integrity of computer based information held within the school or on behalf of the school.
- Safeguards the good standing and legal integrity of the school in terms of computer based information that is held publicly.

The school network

The make-up of the school network
The school network consists of a collection of PC's connected together via Local Area Network (LAN) cabling to a Windows 2008 file server. A gateway to the Cambridgeshire County Council portal further enhances this network. The system runs various levels of software designed to provide security. There are a number of other computers e.g. laptops in school which are not permanently connected to the network, but which are considered to be within the scope of this policy as regards acceptable use.

Legitimate users
Legitimate users of the school network are:

- Current pupils/adult learners
- All teaching staff, Teaching Assistants and support workers
- Office personnel
- School Business Manager
- Therapists
- IT Technicians
- Governors (only using an in-house specified device)

- Parents, when specifically authorised and supervised by a member of staff.
- Visitors, when specifically authorised and supervised by a member of staff e.g. Local Authority officers, software engineers from support companies, community users.
  It is not envisaged that the system will be available for use by, for example, former pupils or cleaning staff.

Legitimate use

The network is designed specifically for educational use. This includes:
- Access to educational and administrative software packages
- Access to reference sources and the sharing of information within the school and outside.
- The storage of information, teaching materials and work products related to educational topics
- Communications between people inside and outside the school for educational ends.

It is intended that the network be used right across the curriculum, not just for the ICT curriculum area, and also for administrative support to staff.
It is also envisaged that the network may be used for personal use in an endeavour to develop the general ICT experience and the continued professional development of both pupils and staff*, but with the following provisos:*

- Personal use of the network must not involve the storage of information that would necessitate the registration of that data under the Data Protection Act. An example of this would be lists of personal data containing more than very basic attributes, e.g. a sports club subscriptions list.
- Personal use of the network must not in any way interfere with normal school operations. For example teaching staff and pupils should not be making personal use of the network during lesson time. Also personal use must not significantly impair the performance of the network or cause excessive amounts of resources to be used, especially photographs, printer ink, paper and disc storage space.
- The network must not be used for commercial use in any way.

Network access control

General comments
The network is to be kept secure using a variety of software products, reviewed regularly, which control access. Individuals gain access through a network wide user-name and password system (referred to as "log-ons"). This system will identify the category of user and the system resources to be made available to that user. *It is not acceptable and is an offence by law to attempt to gain access to another log-on without the permission of that user. Pupils must never be allowed access to staff or system administrator log-ons.*

Connection to the network from outside the school will be allowed to certain named staff. Firewall software is used to ensure that access to the network cannot be gained from outside the school when the network is connected to the Internet; this protection is also is provided via the portal.

Pupils/adult learners
Each pupil/adult learner will have a departmental log-on which they will keep throughout their time within the key stage/provision.

Pupils/adult learners will have access to an area of personal disc space (known as the P: drive) where they can store, edit and delete their work. This area is accessible only by that pupil/adult learners and by staff users. They also have read-only access to a public (pupil templates) area of disk space (known as the Q: drive) from which materials can be copied via year group folders, which gives full public update access to anyone in the year group. This is intended as an area in which collaborative work can take place or where work can be assembled for the teacher to view. *Pupils/adult learners that use this folder need to be aware that they must be careful not to damage or delete the work of others*.

Staff
Each member of teaching staff is assigned an individual log-on. This must be kept secret, especially from pupils/adult learners and outside visitors. Logins are for individual staff only and are not to be shared under any circumstances.

Staff also have full access to an area of personal disc space (known as the H: drive). This is completely private from pupils/adult learners but is accessible by system administrators. Staff have full access to the G: drive and it is here that they can place materials for children/adult learners to view and copy. Disc space named G:/Staff is only accessible by staff. Disc space named J:/curriculum is accessible by staff and administrators. All computers are to be logged out or locked to the individual user when staff leave the room.

System Administrators
The system administrators are a small group of staff, selected by the head teacher, who have overall responsibility for the maintenance and integrity of the network. These will usually include the ICT Administrator and the ICT Technician. They have a set of log-ons that afford full access to the system and all its data, including the ability to change access control. *The passwords for these log-ons must never be divulged to anyone other than the system administrators, the senior management team and engineers from* designated *companies retained to carry out maintenance of the system, without the express permission of the head teacher.*

Virus protection
Computer viruses are items of software that attach themselves to other legitimate items of software or data, without the consent of the computer user, and are programmed to proliferate themselves onto other computers, often to cause disruption or damage. It is essential that all users play a part in protecting the network from the presence of viruses.

It is the policy of the school to run up to date virus protection software on all computers that are attached to the network. This software will automatically report the presence of most known viruses. *Any user who receives an on-screen warning from this software (these are very clear and explicit) should stop all use of the computer immediately and report the occurrence to the ICT Administrator or the ICT Technician.*

Viruses can attach themselves easily to digital media, this is one of the main ways in which they proliferate.

See later sections of this policy regarding Internet use for more details about virus protection considerations.

Internet Access

General
The internet plays an increasingly significant role in the education of the children and adult learners at Highfield and in the professional practice of the staff. For this reason access to the internet is made available from any network computer in the school. However it is recognised that the internet contains material which is unsuitable within a school context or which is offensive. Furthermore the enhanced communications facilities afforded by the internet raise issues of privacy and personal safety. For this reason it is necessary to put in place a range of restrictions on the use of the Internet and all users of the network must be made aware of these.

The network offers the following internet facilities:
- The World Wide Web - i.e. pages of text, images and sound linked together and accessible from computers all over the World.
- Email.

The following internet facilities however are explicitly **not** to be used in school and are masked out by software:
- IRC - Usually known as "Chat rooms". These allow internet users to chat to one another in real time and offer a high degree of anonymity to participants. Whilst there is a place for such a facility in an educational context, the risks inherent in conversations between children and anonymous individuals are much too great for this facility to be offered in its

current form. The availability of more secure and supervised chat facilities will be kept under review.

If you accidentally find a child abuse image do not open it, do not send it on, it is an offence.

- Immediately lock out the computer and contact the ICT Administrator. Ensure no other staff and students have access to the machine.

The World Wide Web

The World Wide Web (WWW) is an invaluable resource for teachers, children and adult learners and its use is to be greatly encouraged in all curriculum areas. However two important usage issues arise:

Finding useful and authoritative materials

The amount of information to be found on the WWW is vast and there are no controls on what is there and how authentic it is. This means that whilst sometimes a rich source of information can be found remarkably quickly, on other occasions hours can be spent in fruitless searching. The ability to sift and search is an essential ICT skill for children/adult learners and needs to be taught specifically. On the other hand, for many internet linked activities, protracted periods of searching will not lend themselves to the main learning objectives of the lesson. *For this reason staff should generally have searched for suitable websites in advance of a lesson and have checked their suitability and accuracy in just the same way as they would do with a book.*

Protection from inappropriate material

The protection of our pupils from inappropriate materials on the WWW is achieved through the use of software and staff supervision. The following measures must be in place:

- Our connection to the WWW must be through an Internet Service Provider that provides a basic level of filtering of inappropriate material.
- The default filtering is via County, which is to the retrospective British Educational Communications & Technology Agency (BECTa) standard.
- Staff need to be active in observing where children/adult learners are browsing on the WWW in case they are moving towards inappropriate areas.
- Any discovery of an unsuitable website should be reported to the ICT Administrator so that the site can be filtered out.
- When asking pupils/adult learners to use search engines to find suitable websites, child oriented search engines such as "Google" or "Ask Jeeves for Kids" should be used as far as possible.
- Children/adult learners are shown how to use ‘advanced’ searches, therefore limiting the chance of finding inappropriate material.

Downloading of materials

The WWW affords many opportunities to download items of data or software free of charge and this material can often be very useful. However caution must be exercised as such downloads can be the source of viruses and other malicious content. The following practices should be followed:

- Children/adult learners should be expected to ask permission before accessing material that requires downloading. There will be appropriate sanctions for pupils/adult learners who are caught downloading inappropriate materials from the Internet or specific mobile devices.
- Staff can download, or allow to be downloaded, the following materials freely:
  -Text (*but not unknown Microsoft Word files*), pictures, databases, etc. that do not contain any executable elements.
  - "Plug-ins" - These are computer programs which extend the ability of a web browser to display different types of graphics and sound. They usually download and install themselves automatically if the user approves. The network will already support the most common plug-ins but new ones must be requested if needed on PC’s or Laptops.
  Importing of files including from unknown or un-trusted origins is not allowed.
- The following materials must be virus-checked by a system administrator before they are used in any way. *<u>Any</u> form of use of these materials before the have been checked could lead to the destruction of large amounts of the school’s data! :*
  - Any executable program.

- Microsoft Office files as these can contain executable elements hidden in the document.

Where staff suspect that they have a problem with their computer or laptop that they have used no data should be transferred and if possible the laptop should not be logged on to the system before talking to the systems administrator.

Supplying personal details
Often websites can ask for personal details to be supplied. For example an educational website might ask for a user's email address so that a regular newsletter can be sent to the user. Staff may supply their individual school email details at their discretion. On the other hand *pupils/adult learners must be taught that they must never supply any details about themselves or the school unless they have consulted a member of staff first*.

E-commerce
E-commerce is a growing area of the WWW and facilitates the buying and selling of goods on-line. No sales or purchases of any kind must be made via the school network except by the school Business Manager, after completion of a school order signed by the budget holder.

Social Media

When using social media for personal use, members of staff must not talk about their professional role in any capacity.

Staff members must not use social media to communicate with any present pupils or any past pupils. In the unlikely event that a member of staff wishes to communicate with a parent of a pupil via social media then this must first be approved by the Head of School or Executive Head in writing.

Members of staff will be instructed to ensure that the maximum privacy settings are set up and maintained on any social media account. They must also only give permission for known friends to access the information on these accounts.

If any member of staff experiences or comes across any derogatory or slanderous comments relating to the school, the academy trust, colleagues or pupils they should take screen shots and pass this onto the e-safety coordinator.

Pupils will receive information and guidance on how to safely use social media.

Note to Parents

- It is written within this policy that no member of staff may be in communication with parents from the school via social media on any platform. Please make this as easy as possible by contacting staff members using the appropriate channels.

Email

Staff email
Every member of the teaching staff is allocated an email address for their professional use. This address uses the registered domain name for the school.

Staff email is web-based rather than held on a mail server in the school so that staff can access their email from home as well as at school.

Pupil/adult learner email
An email account will be provided for some pupils/adult learners in school and there is a class/LINC email account.

Despite these security measures staff must still be sure that they do not accidentally disclose children's/adult learners email addresses to anyone other than legitimate correspondents. For example, do not put up a list of email addresses in a classroom.

It is very important that pupils/adult learners are taught about the dangers of email and reminded of these dangers at the start of each academic year. The issues that should be covered are:

- That the people they are communicating with should be known to them and also to school staff/support workers and/or parents.
- That they should never reply to a message from somebody they do not know and that when they receive such a message they should tell a teacher or their parents immediately.
- That they should report anything they consider to be abusive, upsetting or inappropriate in an email message to a teacher or parent immediately and not respond to the message.
- That they should never give out personal details such as their address or telephone number in an email.
- That their email is not private and that staff and parents must have access to it.
- That they themselves must never include abusive, upsetting or inappropriate material in any message that they send.

Email attachments

- It is possible to attach any number of computer files to an email message. This is very useful and could be used, for example, for a child/adult learners to submit a piece of homework done on a home computer to his or her teacher/support worker. However these attachments do provide another way viruses and other malicious computer code to enter the school's network.
- *For this reason Email users must never open or execute attachments from unknown correspondents.* These should instead be deleted straight away. If staff are at all unsure about other email attachments then they should ask a systems administrator to examine the files and run a virus check if necessary.

School website

In the future editorial control of this website will remain with the Senior Management Team with day to day management of the site being performed by the ICT Administrator, ICT Technician and ICT Co-ordinator. This site will target a wide audience including the pupils/adult learners, parents, staff and governors of the school, other schools and casual visitors from around the world. It aims to have the following content:

- Information for visitors
- Information for parents and prospective parents, including an on-line version of the prospectus and our OFSTED reports.
- Displays of good work from our children
- Curriculum materials and guidance to help our children with homework
- General items of school news including celebrations of success in competitions and fund raising events.
- School Policies

It is the school's policy not to identify the full names of children/adult learners on this website, as a means of protecting privacy. First names only must be used to annotate pictures, good work, sports results, etc. parents will be asked to give or withhold permission for photographs of their children/adult learners to be included in this way in line with the ALT Photograph Policy.

Visitors to the website may be able to contact the school/LINC through email using a feedback form. This saves the school having to publish the school's email address on the site, therefore limiting the amount of spam mail we receive.

School Intranet

The school's curriculum Intranet is available to all staff and can be openly accessed throughout the network. It aims to have the following content:

- Displays of good work.
- Reference materials for children/adult learners in a well-indexed form.
- Teaching activities and resources related to particular year groups.

The Intranet will contain a secure "staff folder" section, accessible via a staff log-on, with the following extra content:

- All policy documents and related materials
- Schemes of Work and Units of Work
- Reference materials

The ICT Administrator will manage the Intranet, but there should be an ethos of openness and joint ownership. Hence all pupils/adult learners and staff are encouraged to produce content and software and make these contents easily available. Because the Intranet is private to the school pupils/adult learners full names can be used openly.

Monitoring and reporting misuse

It is the responsibility of all users of the school's network to report breaches of this Acceptable Use Policy. In addition the system administrators will routinely examine the log files kept by various pieces of network monitoring software to identify potential problems. Examination of staff files and email however will only take place with the permission of the Head Teacher.
Breaches of the Policy should be reported to the ICT Administrator or ICT Co-ordinator in the first instance, who will report to the Senior Management Team if a breach is confirmed. The Senior Management Team will make decisions on appropriate sanctions. Care should be taken with the storage of equipment to reduce the risk of theft or burglary, any equipment left unattended and in plain view should be reported so that it may be stored away safely, especially outside of school/LINC opening hours unless they are secured by specific laptop locks provided by the ICT Administrator.

Security

All ICT equipment will be security marked and noted in the school inventory

- Any equipment taken off site should be signed out by the school administrator
- The administrator and ICT technician will be responsible for regularly updating anti-virus software
- No portable data storage devices from outside school/LINC should be allowed in machines without permission from the ICT Coordinator or ICT Administrator. Encrypted flash drives are supplied to teachers and TA's as necessary.
- Use of ICT will be strictly in line with the school's and LINCS 'Acceptable Use Policy'
- Parents will be made aware of the 'Acceptable Use policy' and will be asked to give signed permission for their children/adult learners to use computers, the Internet and e mail in school /LINC
- All pupils/adult learners and parents will be aware of the School/LINCS Rules for Responsible Use of ICT and the Internet and will understand the consequence of any misuse via the school/LINC agreement on admission and by the availability of policies to read online.
- The agreed rules for Safe and Responsible Use of ICT and the Internet will be included in the school information pack.

Use of cameras and mobile phones

Increasingly technology is making it easier for images to be misused and it is therefore important we take practical steps to ensure that images of children/adult learners taken by staff, parents, carers and by members of the media are done so in a way that is in accordance with the protective ethos of the school/LINC.

Images must be maintained securely for authorised school use only, and disposed of or stored as appropriate in line with the ALT Photograph Policy. We reserve the right to examine any mobile devices and investigate any reports of an infringement of use of school or personal equipment.

- Photos / video can be taken on mobile devices, including phones at celebration events such as Christmas plays and sports days by parents or carers and pupils/adult learners if appropriate. If the school/LINC suspects that the images are to be used inappropriately,

then it must report this on to the appropriate authority. Parents are required to sign a declaration form at each event and agree not to distribute, upload or share images, this includes uploads to social media sites.

- Teachers/support workers may store photographs on laptops. However, they may only be attached to school/LINC documentation and used for school/LINC purposes only. They may not be attached to personal emails or used to advertise your position in school/LINC.

- Any images taken by the media, or for use as publicity etc. must be agreed by the head teacher, clearly stating the intended use for the images before taking them. Having signed a declaration, visitors are allowed to record celebrations etc. but parents of pupils included must be informed and permission sought before publication.

- The use of personal mobile phones and personal mobile devices within school teaching areas (including playgrounds) is strictly prohibited. Under no circumstances are images to be captured or shared. Mobile phones are only to be used in emergency situations when it is a designated point of contact off the school teaching site.

Appendix 1 - The main points that staff need to remember

- Don't divulge your staff log-on password under any circumstances and change it if you think it has been compromised.
- Don't leave a computer unattended and logged on to a staff log-on.
- Make sure that personal use of the network does not interfere with normal school/LINC operations.
- Explicitly teach children/adult learners the points laid out in Appendix 2 i) at the start of each academic year and ii) when relevant computer based activities are about to begin.
- Actively monitor the websites that children/adult learners are visiting during open web-browsing sessions and do not leave a group unsupervised.
- Try wherever possible to visit websites before you use them in your teaching so that you can check their acceptability.
- When children/adult learners are to use a search engine, try to make it one that has been developed for suitable use.
- Report any inappropriate websites that you find to the ICT Co-ordinator/Administrator so that they can be filtered out.
- Never divulge the wifi log-on password, and ask for it to be changed if you think it has been compromised.
- Actively monitor pupils/adult learners' email messages.
- Always respond to an on-screen virus warning. Isolate the machine and inform the ICT Co-ordinator/Administrator immediately.
- If you download any executable programs or Microsoft Word documents, have them virus checked before you open them or execute them. The same applies when this type of file has been emailed to you by someone that you know.
- Never open or execute a file sent to you by someone that you don't know. Delete it immediately.
- Do not buy or sell anything via the school network without the permission of the Head Teacher.
- Do not divulge pupil/adult learners email addresses.
- The use of personal mobile phones and personal mobile devices within school teaching areas (including playgrounds) is **strictly prohibited**. Under no circumstances are images to be captured or shared. Mobile phones are only to be used in emergency situations when it is a designated point of contact off the school teaching site.
- When using social media for personal use, ensure that privacy settings are at a maximum. Do not discuss anything to do with school or your role; do not become “friends” or “follower” (ie communicate with) of any current pupils or past pupils under 18. The same applies to parents/carers of current students. If you see anything derogatory related to the school, report it to the Head of School.

Appendix 2 - What pupils/adult learners are taught about acceptable use of IT

These teaching points are modified dependent on the age/ability of the children/adult learners and the extent of their use of the network.

- Always log off when you have finished using a computer.
- Never disclose your password.
- Do not log-on as anyone else.
- If you get a message on the screen about a virus, stop working and tell a teacher/support worker straight away.
- Don't put portable data storage devices from home into the school's computers. If you want to use one, discuss it with a teacher/support worker.
- If you see anything on the Internet that you think is upsetting or rude inform the teacher/support worker straightaway.
- Do not give your email address to anybody, particularly a stranger, without asking your teacher/support worker first.
- Never type your name, address or other personal details in on a web page without asking permission first.
- If you receive an email from somebody that you don't know, tell a teacher/support worker as soon as possible.
- Never tell anyone private details about yourself in an email, especially your address and telephone number.
- Remember the rules about being kind and considerate in what we say to others applies to email as well.
- Be aware that their email is not private and that teachers/support workers may look at what they have written.
- Be aware that the network can detect misuse of the computers and record details of the person responsible.
- Never download files or programs from the Internet without getting permission from a teacher/support worker.
- Tell a teacher/support worker about any files attached to an email that you were not expecting to receive.
- Be careful not to change or delete other people's work in the P:\Shared Files folder.

ACCEPTABLE USE OF INTERNET

- All potential users of the Internet should understand basic conventions and navigation techniques before going on-line and accessing Web pages.
- We will inform children/adult learners that logs are kept of sites visited and why. Children/adult learners should report any cyber-bullying to a member of staff who will be able to follow the trail
- Children/adult learners must agree to act responsibly and use the Internet in school/LINC for course-related work only
- Children/adult learners must agree to respect copyright and not to plagiarize others' work
- Children/adult learners must agree to download pages only to the disk specified by the teacher/support worker. We will explain why such restrictions are necessary
- Members of staff will check personal disks and mobile devices for viruses and unsuitable material
- Children/adult learners must agree not to attempt to access unsuitable material
- We will remind children/adult learners that the possession of certain types of unsuitable material can lead to prosecution by the police

Sanctions for violations of the Acceptable Use Policy
Minor infringements will be dealt with by enforcing a temporary ban on Internet use and / or by additional disciplinary action in accordance with existing academy procedures and policies. For serious or repeated minor violations, the child/adult learner's parents will be involved.

The Internet at home
Parents are expected to discuss and agree some sensible points with their children. We suggest they:

- keep in touch with what children/adult learners are doing with their computers,
- ask them to show which sites they have visited and talk about what they learned there
- encourage children/adult learners to use computers, phones and tablets only as one of a range of other activities.
- Ensure that all social media has the highest possible privacy settings and that pupils/adult learners are only in contact with 'real' friends.

Parents are strongly advised to:

- Keep use of all internet accessible devices such as phones, tablets and laptops restricted to a place where a responsible adult can supervise
- Be aware that devices are not limited to those mentioned above. Gaming machines also allow online communication.
- Take an interest in what children/adult learners are doing with the computer and install '*Hector the Protector'* monitoring device on www.microsoft.com
- Ask children/adult learners to show how the family computer works and explain how they use computers at Highfield and LINC
- Advise children/adult learners to take care whenever they are on-line reminding them never to give out any personal information about themselves, particularly full, names, addresses, phone numbers, or financial information.
- Remind children/adult learners never to give anyone else their password
- Remind children/adult learners that people on-line may not be who they seem, and no matter how well they feel they know someone, ***that person is still a stranger***
- Ensure that children and adult learners never arrange to meet someone in person that they have made contact with on-line
- Tell children and young adults to inform a member of staff/family member who will delete attachments from strangers without opening them; they may contain viruses that can damage the computer

- Tell children and young adults not to respond if they see any messages which they find upsetting, and reinforce that emails. They should tell a member of staff/family member about any such messages.
- Emails offering banking and/or prizes are from people they don't know and therefore shouldn't be responded to. They should tell a member of staff/family member about any such messages.
- Make sure that using social media and playing video games are only two activities among many that you can enjoy.
- Be aware that children/adult learners with access to credit cards could use them for on-line purchases, if not supervised
- Learn at least the basics about computers if not computer literate

The following letter is sent out to parent and carers of any new students/ adult learners to the school.

Dear Parent/Carer

Use of Internet by Pupils

To support learning opportunities within the academy, students and adult learners may be given access to the internet as information and research source and a communications tool.

The internet is a major source of educationally useful material and the primary distribution medium for a wide range of organisations. The potential to support the classroom teacher, LINC manager and support workers and the learner is significant and will continue to grow.

There are well publicised concerns regarding access to material on the internet that would be unsuitable for students/adult learners. Whilst it is impossible to ensure that a student/adult learner will not access such material, the academy is taking all reasonable steps to minimise students and adult learners' access to unsuitable material. These include:

- *Use of a filtered internet service to prevent access to internet sites with undesirable material*
- *The requirement that wherever possible, all internet access during school/LINC hours will be supervised by a member of staff or another responsible adult*
- *Education of students/adult learners as to the potential legal consequences of accessing certain types of materials.*

In addition to the above, adult learners are taught safe and appropriate behaviour around the internet and social media. I have included below a copy of the form that we use to record which students/adult learners have received lessons on in-school internet safety.

Authorised Use consent form for pupils

- *Always log off when you have finished using a computer.*
- *Never disclose your password.*
- *Do not log-on as anyone else.*
- *If you get a message on the screen about a virus, stop working and tell a support worker straight away.*

- *Don't put portable data storage devices such as memory sticks from home into the provisions computers. If you want to use one, discuss it with a support worker.*
- *If you see anything on the Internet that you think is upsetting or rude, use Hector the Protector and show it to an adult who will inform the provision manager straightaway.*
- *Do not give your email address to anybody, particularly a stranger, without asking your teacher/support worker first.*
- *Never type your name, address or other personal details in on a web page without asking permission first.*
- *If you receive an email from somebody that you don't know, tell a teacher/support worker straight away.*
- *Never tell anyone private details about yourself in an email, especially your address and telephone number.*
- *Remember that the academy rules about being kind and considerate in what we say to others applies to email as well.*
- *Be aware that your email is not private and that teachers/support workers may look at what you have written.*
- *Be aware that the network can detect misuse of the computers and record details of the person responsible.*
- *Never download files or programs from the Internet without getting permission from a teacher/support worker.*
- *Tell a teacher/support worker about any files attached to an email that you were not expecting to receive.*
- *Be careful not to change or delete other people's work in the T:\Shared Files folder.*

Our staff must also follow strict rules and I would like to bring to your attention the following excerpt from the policy.

> *''When using social media for personal use, ensure that privacy settings are at a maximum. Do not discuss anything to do with school or your role; do not become "friends with" or "follower of" (ie communicate with) any current pupils or past pupils. The same applies to parents/carers of current students"*

Taking the above into account, please remember that the best ways to communicate with support staff are through Class Dojo, the contact diary, by telephone or by making an appointment to see them in person.

Finally, I wanted to share with you a part of our "Acceptable Use of IT" policy. This part is aimed at parents and carers and is largely common sense advice, but I hope it proves useful.

The Internet at home

Parents and carers should discuss and agree some sensible points with their children and adult learners. We suggest they:

- *keep in touch with what children and adult learners are doing with their computers,*
- *ask them to show which sites they have visited and talk about what they learned there*
- *encourage children and adult learners to use computers, phones and tablets only as one of a range of activities.*
- *ensure that all social media has the highest possible privacy settings and that pupils and adult learners are only in contact with 'real' friends.*

Parents are strongly advised to:

- *Keep use of all internet accessible devices such as phones, tablets and laptops restricted to a place where an adult/responsible person can supervise*

- *Be aware that devices are not limited to those mentioned above. Most gaming machines also allow online communication.*
- *Take an interest in what children and adult learners are doing with the computer and install 'Hector the Protector' monitoring device on www.microsoft.com*
- *Ask children and adult learners to show how the family computer works and explain how they use computers at Highfield*
- *Advise children and adult learners to take care whenever they are on-line reminding them never to give out any personal information about themselves, particularly full, names, addresses, phone numbers, or financial information.*
- *Remind children and adult learners never to give anyone else their password*
- *Remind children and adult learners that people on-line may not be who they seem, and no matter how well they feel they know someone,* ***that person is still a stranger***
- *Ensure that children and adult learners never arrange to meet someone in person that they have made contact with on-line*
- *Tell students and adult learners to inform a member of staff/family member who will delete attachments from strangers without opening them; they may contain viruses that can damage the computer*
- *Tell students and adult learners not to respond if they see any messages which they find upsetting, and reinforce that emails. They should tell a member of staff/family member about any such messages.*
- *Emails offering banking and/or prizes are from people they don't know and therefore shouldn't be responded to. They should tell a member of staff/family member about any such messages.*
- *Make sure that using social media and playing video games are only two activities among many that children and adult learners can enjoy.*
- *Be aware anyone with access to credit cards could use them for on-line purchases, if not supervised*
- *Learn at least the basics about computers if not computer literate*

Many thanks for taking the time to read this lengthy letter; I do hope that it gives you a better picture of some of the precautions we take to keep all of our students and adult learners safe. Please don't hesitate to contact me if you have any questions or comments about any of the above. Please can I ask that you sign and return the slip below to indicate that you have read and understood and consent to us using the internet carefully.

With kind regards

Adam Daw
Head of School

I confirm that I understand Highfield Ely Academy's approach to the acceptable use of ICT and consent to accessing the internet with supervision at LINC 19-25

Adult learners name: _____

Parent/Carer (print name): _____

Parent/Carer (sign): _____

Adult learners who are going to be accessing ICT devices that are internet capable must understand and sign the following form when they join the school or start using such devices.

Authorised Use consent form for adult learners

The academy has adopted certain safeguards in order to minimise any risk to adult learners. Please read through these points and sign below.

- *Always log off when you have finished using a computer.*
- *Never disclose your password.*
- *Do not log-on as anyone else.*
- *If you get a message on the screen about a virus, stop working and tell a support worker straight away.*
- *Don't put portable data storage devices such as memory sticks from home into the academies computers. If you want to use one, discuss it with a teacher.*
- *If you see anything on the internet that you think is upsetting or rude, use Hector the Protector and show it to an adult who will inform the provision manager straightaway.*
- *Do not give your email address to anybody, particularly a stranger, without asking your support worker first.*
- *Never type your name, address or other personal details in on a web page without asking permission first.*
- *If you receive an email from somebody that you don't know, tell a support worker straight away.*
- *Never tell anyone private details about yourself in an email, especially your address and telephone number.*
- *Remember that the academy rules about being kind and considerate in what we say to others applies to email as well.*
- *Be aware that your email is not private and that support workers may look at what you have written.*
- *Be aware that the network can detect misuse of the computers and record details of the person responsible.*
- *Never download files or programs from the Internet without getting permission from a support worker.*
- *Tell a support worker about any files attached to an email that you were not expecting to receive.*
- *Be careful not to change or delete other people's work in the T:\Shared Files folder.*

Date……

Adult learner ……

All new staff must sign the following form.

Authorised Use consent form for staff

The academy has adopted certain safeguards in order to minimise any risk to staff and adult learners. The main points are detailed below. Once you have read these please sign below for our files.

- Don't divulge your staff log-on password under any circumstances and change it if you think it has been compromised.
- Don't leave a computer unattended and logged on to a staff log-on.
- Make sure that personal use of the network does not interfere with normal school operations.
- Explicitly advise adult learners the points laid out in Appendix 2 i) at the start of each academic year and ii) when relevant computer based activities are about to begin.
- Actively monitor the websites that adult learners are visiting during open web-browsing sessions and do not leave a group unsupervised.
- Try wherever possible to visit websites before you use them in your teaching so that you can check their acceptability.
- When adult learners are to use a search engine, try to make it one that has been developed for appropriate use.
- Report any inappropriate websites that you find to the ICT Co-ordinator/Administrator so that they can be filtered out.
- Never divulge the "www" log-on password, and always ask for it to be changed if you think it has been compromised.
- Actively monitor adult learners email messages.
- Always respond to an on-screen virus warning. Isolate the machine and inform the ICT Co-ordinator/Administrator immediately.
- If you download any executable programs or Microsoft Word documents, have them virus checked before you open them or execute them. The same applies when this type of file has been emailed to you by someone that you know.
- Never open or execute a file sent to you by someone that you don't know. Delete it immediately.
- Do not buy or sell anything via the school network without the permission of the Head Teacher.
- Do not use personal mobile phones and personal mobile devices within Academy teaching areas (including playgrounds/outside spaces), this is **strictly prohibited**. Under no circumstances are images to be captured or shared. Mobile phones are only to be used in emergency situations when it is a designated point of contact off the Academy teaching site.

Name…….. Date……