ICT AND USE OF THE INTERNET AND INTRANET BY STAFF POLICY

Reviewed and updated: March 2022
Next review: March 2025
Status: non-statutory

This policy should be read in conjunction with the following policies:

- E-safety
- Staff email.
- Social media.
- Internal data security.
- Management and retention of records.
- Staff professional identity protection.
- Use of personally owned devices by staff.

Background

Information and Communications Technology (ICT) is a vital tool in the process of teaching and learning. Teachers prepare pupils through ICT for a rapidly changing world in which many activities are transformed by access to a varied and constantly changing and developing technology.

Pupils use ICT tools to find and process information and teachers need to set an example of how this is done in a responsible manner, creatively and with discrimination. Pupils learn from teachers how to employ ICT to enable rapid access to ideas and experiences from a wide range of sources. All staff need to become confident users of ICT, so that they can develop the skills, knowledge and understanding which enables them to use appropriate ICT resources effectively as powerful tools for teaching.

ICT is also a vital tool in the administration of the school. Teachers and support staff need to be aware of what is acceptable use of the school's administrative network of computers, including in relation to data protection and the General Data Protection Regulation (GDPR).

ICT AND USE OF THE INTERNET AND INTRANET BY STAFF POLICY

AT ELTHORNE PARH HIGH SCHOOL

ALL OUR SYSTEMS ARE CLOSELY MONITORED

Introduction

This policy is in place for use of these facilities by staff. There is a separate policy for use by pupils.

There is a small network of computers which are used in the administration of the school (finances, pupil records, timetables, registers etc). Many more computers are available for use by pupils and staff and the majority of these have access to the internet through the school network. All pupils and staff have a login name, password and an email account.

The email system is available for use both from within the school and externally using a web browser. There are specialist IT rooms and some general-purpose IT and private study rooms. A growing number of other laptop computers are located within individual departments/classroom areas.

Objectives and targets

The objective of this policy is to develop an appropriate code of practice for use of ICT by staff at **Elthorne Park High school.**

Action plan

Responsibilities of the school
The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another's files without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's internal data security policy and as required by the General Data Protection Regulation (GDPR).
- Logs are maintained of access by users and of their actions while users of the system.
- Logs are also maintained of access under the use of personally owned ICT devices by staff policy.

Rights of access

- A safe and secure username/password system is essential and will apply to all school ICT systems, including email and virtual learning environment (VLE).

- All passwords are generated by the network manager/ICT technical support staff and are unique to each member of staff. Passwords can only be reset by the user or by the ICT technical team. All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the network manager and these will be reviewed, at least annually.

- The 'master/administrator' passwords for the school ICT system used by the network manager/ICT technical support team are also available to the headteacher or other nominated senior leaders and kept in a secure place (e.g. school safe). In the event of a serious security incident, the police may request, and will be allowed access to, passwords used for encryption.

Emails

- The computer resources at **Elthorne Park High** school belong to the school and are to be used solely for educational or business purposes, although the governors will permit limited use for personal purposes, provided that it does not interfere with work performance and provided that rules of usage are observed.

- Email is an essential tool at the school and all members of staff must read and abide by the separate staff email policy when managing their email accounts, sending emails, receiving emails and especially if emailing personal, sensitive, confidential or classified information covered by the GDPR.

- The school reserves the right to intercept, monitor, analyse and read all email generated, received or distributed via the school networks, equipment and email addresses.

Internet and intranet

- Known pornographic sites on the internet are blocked and filters to intercept prohibited material and offensive language are in place. The internet is not necessarily secure and staff need to be aware that school sensitive information could be viewed by unauthorised individuals.

Digital images

- When using digital images, staff inform and educate pupils about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognise the risks attached to publishing their own images on the internet e.g. on social networking sites. Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images [see the e-safety policy]. Any images should only be taken on school equipment. Personal equipment of staff should *not* be used for such purposes.

Portable ICT equipment

- Laptops, ipads, tablets and similar devices which are the property of the school fall under the same restrictions of use as networked computers. Serious misuse of such equipment will be treated as a disciplinary offence and may result in dismissal. Loss, damage or theft of school equipment through misuse, or negligence may result in financial sanctions.

- All school-supplied portable ICT equipment should be kept in a secure place and transported in the car boot. When not in use, they should be switched off and securely stored.

- Laptops and other devices that are the personal property of the individual must only be used in line with the use of personally owned devices by staff policy. [See the Use of personally owned ICT devices by staff (BYOD)].

Code of practice to be adhered to by staff

- All staff will be expected to sign the acceptable computer usage agreement – see appendix 1.

- Staff who receive portable ICT equipment, such as a laptop or tablet, which is the property of the school will also be expected to sign the acceptable portable ICT equipment usage agreement – see appendix 2.

- Staff who bring into school their own devices (BYOD), ie ICT devices not issued by the school, will also be expected to sign the acceptable BYOD usage agreement – see appendix 3.

- The ordering/purchasing of goods over the internet is subject to the same authorisation procedures and limits as purchases made by other means and failure to follow the correct procedure may result in disciplinary action.

- Under the government’s prevent legislation, schools are required to demonstrate that they are protecting children from being drawn into terrorism. Any member of staff suspecting that pupils may be viewing or visiting suspicious websites should advise the headteacher immediately so that the local authority (LA) can be alerted and the matter taken forward if necessary.

- Staff must abide by the current restrictions on correspondence or the passing of information to outside organisations or individuals.

Note. There have been many instances reported of electronic communication systems, and their output, challenging the professionalism of school staff. Colleagues should be guarded in their use of all such systems.

Misuse of computer systems by staff

Misuse or abuse of computer systems by staff is a serious matter and will be dealt with under the school’s disciplinary procedures. The penalties for improper use may include dismissal either with or without notice.

- The transmission of school sensitive data over the internet is strictly prohibited.

- Staff may not use the internet in a role inconsistent with their role in the school.

- At no time may staff use the internet to send school or personal information that would, if intercepted, place the school in violation of UK laws or regulations.

- Staff may not use the internet to view, download or forward illegal, pornographic, racist, inflammatory or seditious material that would place the school at legal risk.

- Staff must not gain unauthorised access to the internet e.g. by hacking or by trying to circumvent any ‘blocking’ controls. Hacking into computers is a criminal offence and they could be prosecuted under the Computer Misuse Act 1990.

- Staff must not engage inappropriately with pupils through social networking sites. Staff must be mindful that all postings on social network sites are widely accessible. [See also the social media policy].

- Staff must not engage in sending or forwarding abusive or offensive emails – inside or outside the school – or material that could cause offence. This applies to all email, whether intended for person-to-person communication or wider distribution.

- Staff may not download or distribute material from the internet without virus checking. Users are responsible for virus checking any material.

- Staff must not use another individual’s user identity to access the internet or intranet.

- Staff may not download screensavers, sounds, images, or audio-visual materials for storage on local PCs.

- Staff may not use the internet for private business purposes or private commercial gain.

- Staff may not export or transmit school software via the internet without authorisation.

- Staff may not upload, download or forward games software.

- Staff may not generate or forward ‘chain’ messages or letters.

The list may be added to at any time.

Any queries regarding this policy should be addressed to the headteacher.

Monitoring and evaluation

All use of the internet is recorded and the headteacher may request access to internet logs, emailing history etc if the senior management team considers that this policy has been contravened, in order to investigate alleged abuse. The policy itself will be monitored and evaluated regularly taking into account any incidents which occur or technological developments which might need a change in the policy.

Reviewing

The efficacy of the policy will be discussed annually as part of the governors’ rolling programme of reviews.

Next school review due: March 2025

APPENDIX 1

Acceptable computer usage agreement

- I acknowledge that the computer provided for me to use remains the property of the school and should only be used for school business.
- I will only access the system with my assigned login name and registered password.
- Passwords that I use to access school systems will be kept secure and secret.
- If I have reason to believe my password is no longer secure I will change it immediately. I will inform the network manager as soon as possible so that any access with my old password can be monitored and appropriate action taken.
- I understand that I am allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Any images will only be taken on school equipment, never on personal equipment.
- If I use removable media I will ensure that this has been carefully checked to ensure it is free from any type of virus.
- I will follow the guidance provided by ICT support staff to ensure the anti-virus protection on my computer is kept up-to-date.
- I will check with the network manager/technician should I need to install additional software.
- **I will always adhere to the following associated school policies:**

o E-safety policy.

o Staff professional identity policy.

o Internal data security policy.

o ICT and use of the internet and intranet by staff.

o Staff email policy and procedures.

o Social media policy.

o Use of personally owned ICT devices by staff.

- I will always adhere to copyright.
- I will always log off the system when I have finished working.
- I understand that the school may monitor the websites I visit.
- I understand that a criminal offence may be committed by deliberately accessing websites that contain certain illegal material.

- I understand that staff are not permitted to access social media websites from the school's computers, staff laptop or other school device at any time unless authorised to do so by a member of the senior management team.

- I will only open email attachments when I am sure that they come from a recognised and reputable source. I will bring any other attachments to the attention of the network manager/headteacher/ designated safeguarding lead.

- Any email messages I send will not damage the reputation of the school. All joke emails and attachments are potentially damaging and undesirable and therefore will not be used.

- I will report immediately to the headteacher any unpleasant material or messages sent to me.

- I understand that use of the school's equipment for personal financial gain, gambling, political purposes or advertising is forbidden.

- I understand that storage of emails and attachments should be kept to a minimum to avoid unnecessary drain on memory and capacity.

- I understand that activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.

- I understand that I am responsible for the safety of sensitive school data that I use or access.

- In order to maintain the security of data I will take the following steps:

○ I will store data files in my user area only for as long as is necessary for me to carry out my professional duties.

○ I will only save data files to a computer, laptop or other ICT equipment that is provided by the school.

○ If I need to transfer data files, I will only do so using the encrypted USB key provided by the school.

○ I will not share or give out any passwords that I use to access school systems. If I have reason to believe that my password is no longer secure I will change it.

○ I will not use email to transfer data files but save them to the school network area if other staff need access to the information.

o If I am in any doubt as to the sensitivity of data I am using I will refer to the school's internal data security policy to check. (Sensitive data could include pupil reports, SEN records, letters to parents, class-based assessments, exam results, whole school data, medical information, and information relating to staff eg performance reviews).

- I will not access the files of others or attempt to alter the computer settings.

- I will not update web logs or use pictures or text that can identify the school without the permission of the headteacher.

- I will not alter, attempt to repair or interfere with the components, software or peripherals of any computer that is the property of the school.
- I will not post anonymous messages or forward chain letters.
- I understand that if I do not adhere to the rules outlined in this agreement, my network access could be suspended and that other disciplinary consequences may follow, including notification to professional bodies, where appropriate.
- I understand that if an incident is considered to be an offence under the Computer Misuse Act this may require investigation by the police and could be recorded on any future criminal record checks.
- I understand that if an incident is considered to be a breach under the Data Protection Act or the General Data Protection Regulation (GDPR) this may require investigation by the Information Commissioner's Office and heavy financial or other sanctions could apply to the school.

Name………………………………….

Date…………………………………..

APPENDIX 2

Acceptable portable ICT equipment usage agreement

- The [laptop/ipad/tablet] is the property of **Elthorne Park High** school. It has been allocated to me as a member of staff and is my responsibility. If another member of staff borrows it, the responsibility still stays with me and I understand that only school staff may use the equipment.

- I understand that students must never use the equipment.

- When I leave the school's employment, the equipment will be returned to the school. Should I be on extended leave of four weeks or more I will return the equipment to the school (unless I have a prior agreement with the headteacher).

- I understand that when in school and not being used, the equipment must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.

- I understand that, whenever possible, the equipment must not be left in an unattended car. If there is a need to do so, it will be locked in the boot.

- I will check that the equipment is covered by my normal household insurance. If this is not the case, then either the insurance must be changed or the equipment should be kept in school and locked up overnight.

- I understand that the equipment must not be taken abroad, other than as part of a school trip, and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.

- I understand that when being transported, the carrying case supplied must be used at all times.

- I understand that I have the responsibility to ensure the virus protection software that has been installed on the equipment is kept up-to-date. I also understand that I must *always* follow the virus protection procedures as directed by the school's technical support provider/network manager to ensure virus protection is always kept up-to-date.

- I understand that I should not attempt to significantly alter the computer settings other than to personalise my desktop working area.

If you are unsure about any of the asterisked * points below you must consult the network manager.

- I understand that I may load software onto the equipment but it must:

o Be fully licensed*.

o Not corrupt any software or systems already installed on the equipment.*

o Not affect the integrity of the school networks when connected to either the curriculum or administration networks.*

- I understand that if I use any removable medium then it must be checked to ensure it is free from any viruses.*
- If any fault occurs with the equipment I will refer it immediately to the technical support staff/network manager.
- If I am in any doubt as to the sensitivity of data I am working on when using portable ICT equipment supplied by the school I will refer to the school's internal data security policy to check. (Sensitive data could include pupil reports, SEN records, letters to parents, class-based assessments, exam results, whole school data, medical information, and information relating to staff, eg performance reviews).
- I understand that if I do not adhere to these rules outlined in this agreement, my network access could be suspended and that other disciplinary consequences may follow, including notification to professional bodies, where appropriate.
- I understand that if an incident is considered to be an offence under the Computer Misuse Act this may require investigation by the police and could be recorded on any future criminal record checks.
- I understand that if an incident is considered to be a breach under the Data Protection Act or the General Data Protection Regulation (GDPR) this may require investigation by the Information Commissioner's Office and heavy financial or other sanctions could apply to the school.

Equipment issued to ___________________________ on __________________________________

Staff name _________________________________ Network support ________________________

APPENDIX 3

ACCEPTABLE BYOD USAGE AGREEMENT

- I understand that anyone other than myself must never have access to any sensitive data held on the bring your own device (BYOD).
- I understand that I am responsible for the safety of sensitive school data that I use or access.
- All personal data is subject to the General Data Protection Regulation (GDPR) and if I am in any doubt as to the sensitivity of data I am using, I will refer to the school's internal data security policy, and to the data protection officer if still unsure. I understand that if an incident is considered to be a breach under the Data Protection Act or the GDPR this may require investigation by the Information Commissioner's Office and heavy financial or other sanctions could apply to the school.
- I will always adhere to copyright.
- I will always log off the system when I have finished working.
- I will only access the school's systems with my assigned login name and registered password.
- Passwords that I use to access school systems will be kept secure and secret.
- If I have reason to believe my password is no longer secure, I will change it immediately. I will inform the network manager as soon as possible so that any access with my old password can be monitored and appropriate action taken.
- When I leave the school's employment, all data relating to the school will be returned to the school.
- I understand that when in school and not being used, the BYOD must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.
- I understand that, whenever possible, the BYOD must not be left in an unattended car. If there is a need to do so, it will be locked in the boot.
- I will check that the BYOD is covered by my normal household insurance, whether in England or abroad.
- I understand that I have the responsibility to ensure the virus protection software that has been installed is kept up-to-date. I also understand that I must *always* follow the virus protection procedures as directed by the school's network manager to ensure virus protection is always kept up-to-date.
- I will follow the guidance provided by ICT support staff to ensure the anti-virus protection on my BYOD is kept up-to-date.
- If I use removable media I will ensure that this has been carefully checked to ensure it is free from any type of virus.

- I understand that I may load software onto the BYOD but it must:
  - Be fully licensed.
  - Not corrupt any software or systems already installed on the BYOD.
  - Not affect the integrity of the school networks when connected to either the curriculum or administration networks.
- I will check with the network manager/technician should I need to install additional software.
- **I will always adhere to the following associated school policies:**
  - E-safety
  - ICT and use of the internet and intranet by staff.
  - Use of personally owned ICT devices by staff (BYOD).
  - Management and retention of records.
  - Internal data security policy.
  - Social media.
  - Staff email.
  - Staff professional identity protection.
- I understand that the school may monitor my BYOD activity.
- I understand that members of staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. I understand that such images must only be taken on school equipment, never on personal equipment.
- I understand that activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- In order to maintain the security of data, I will take the following steps:
  - I will store data only for as long as is necessary for me to carry out my professional duties.
  - If I need to transfer data files, I will only do so using encryption as advised by the network manager.
  - I will not use email to transfer data files but save them to the school network area if other staff need access to the information.

I understand that if I do not adhere to these rules outlined in this agreement, my privilege of working with the BYOD could be suspended and other disciplinary consequences may follow, including notification to professional bodies, where appropriate.

If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may require investigation by the police and could be recorded on any future criminal record checks. Breaches of the GDPR may cause the school significant financial penalties.

Name………………………………….

Date…………………………………..