ICT & E-SAFETY POLICY

This policy was created and ratified by the Trust Board in:	**May 2018**
The policy owner is:	**Director of Data**
This policy will be reviewed by the Trust Board in: (unless earlier review is recommended by the Trust)	**May 2021**
Policy Version:	**V1.0**

1. <u>Why is the use of the Internet Important?</u>

The internet is an essential element in twenty-first century life for education, business and social interaction. It is an open communications channel allowing information to be transmitted to many locations in the world. Messages may be sent, ideas discussed and material published with very little restriction. These features of the internet make it an invaluable resource used by millions of people every day. The purposes of Internet use in school are to promote student achievement, to support the professional work of staff and to enhance the school's management, information and business administration systems.

Benefits of using the internet and web services in education include:

- Access to world-wide educational resources
- Educational and cultural exchanges between children world-wide
- Cultural, vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for children and staff
- Staff professional development through access to national developments, educational materials and good curriculum practice
- Communication with support services, professional associations and colleagues
- Improved access to technical support including remote management of networks
- Exchange of curriculum and administration data with Children's Services and DfE

The statutory curriculum requires children to learn how to locate, retrieve and exchange information using ICT. Consequently, in delivering the curriculum teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail to enrich and extend learning activities. Effective internet use is an essential life skill for all children to master.

2. Core Principles of Internet Safety

In common with most technologies, internet use presents risks as well as benefits. Children could be placed in inappropriate and even dangerous situations without mediated internet access. To ensure responsible use and the safety of children the school's policy is built on the following five core principles.

2.1 Guided Educational Use

Internet use will be planned, task orientated and educational within a regulated and managed environment.

2.2 Risk Assessment

Both staff and children will be aware of the risks associated with internet use. Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school allowed. Staff and children will know what to do if they come across inappropriate material when using the internet.

2.3 Responsibility

Internet safety depends on staff, governors, advisors, parents and children themselves taking responsibility for use of the internet and associated technologies. The school will seek to balance education for responsible use, regulation and technical solutions to ensure children's safety.

2.4 Regulation

The use of the internet, which brings with it the possibility of misuse, will be regulated. (Internet Use Code of Practice – Appendix 1)

2.5 Appropriate Strategies

Effective, monitored strategies will be in place to ensure responsible and safe internet use. The school will work in partnership with the Children's Services, the Department for Education, parents and the Internet Service Provider to ensure systems to protect children are regularly reviewed and improved.

The ICT Services Manager/Network Manager will be designated as E-Safety Coordinator. The E-Safety coordinator and the Headteacher will'.

- Maintain an e-safe culture
- Act as a key point of contact on all E-Safety issues
- Raise awareness and understanding of E-Safety to all stakeholders, including parents and carers
- Embed E-Safety in staff training, continuing professional development and across the curriculum and learning activities
- Maintain an E-Safety incident log and report on issues
- Understand the relevant legislation
- Liaise with the local authority and other agencies as appropriate
- Review and update E-Safety policies and procedures regularly

The Wensum Trust E-Safety policy is based on the Norfolk E-Safety Policy and government guidance.

3. Internet Access

3.1 Children

Parents will be informed that children will be provided with monitored internet access and will be required to sign the code of conduct acknowledging their understanding of the School's policy and internet and network use. The school will keep a record of all children who are granted internet access. The record will be monitored by the ICT Services Manager/Network Manager.

3.2 Staff, Governors and Community

Use of network and internet services by Staff and Governors is covered by the Local Authority policy (see guidance note P319 via Schools PeopleNet), including the use of public social networking sites such as Facebook, Instagram, Twitter etc.

All staff must read and sign the Staff Code of Conduct before using any school ICT resource (Appendix 3).

The following rules apply to all network users including those from the Community and Extended Services:

- I will only access the system with my own login and password, which I will keep secret
- School computer and internet use must be for educational activities
- The copyright and intellectual property rights of others must be respected
- Users must not bring in offensive material via memory devices, the internet or an e-mail attachment
- Users are responsible for not spreading offensive material across the network or internet
- Anonymous messages and chain letters must not be sent
- Irresponsible use of the network for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- The school may exercise its right by electronic means to monitor the use of the school network, including web-sites and e-mails. The school may delete inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal or unsuitable purposes.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for children. The school, with the support and guidance of Children's Services, will take all precautions to ensure that users only access appropriate material. However, due to the international and linked nature of internet content, it is not possible to guarantee that unsuitable material will never occur on a school computer. Neither the school nor Norfolk Children's Services can accept liability for the material accessed, or any consequences of internet access.

If staff or children accidentally discover unsuitable sites, the URL (address) and content must be reported immediately to the ICT Services Manager/Network Manager who will make the necessary adjustments to the school's filtering arrangements and/or advise the service provider. Staff and children will be made aware that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

4. Copyright Law

The use of internet derived material by staff and pupils must comply with copyright law. Guidance is available from several sources, principally the Copyright Licensing Agency http://www.cla.co.uk/. Many websites will include a copyright statement setting out exactly the way in which materials on the site may be used. When using websites in school, children and staff should be encouraged to look for copyright information, so reinforcing their understanding of the importance of this issue.

5. School Websites

The contact details on the school web site will be the school address and other agreed details, no staff or student personal information will be published.

6. Publishing Children' Images and Work

Photographs that include children will be selected carefully and will not enable individual children to be clearly recognised unless express permission has been given by an adult with parental responsibility. This permission is requested when each student joins the school and is recorded onto the school database. Full names will not be used in association with photographs.

7. E-mail

Each member of staff will have their own e-mail address provided by the school, which can be accessed both at school and off-site. Children must not reveal details of themselves or others, such as their address or telephone number, or arrange to meet anyone in e-mail communication without specific permission.

Children must immediately tell a teacher if they receive offensive e-mail.

Staff must report reception of offensive or inappropriate e-mails to the ICT Services Manager/Network Manager.

Staff must use their school provided e-mail address when communicating with children and parents.

8. Blogging and other forms of Social Networking / Collaborative Working / YouTube / Newsgroups

It is a requirement of some exam syllabuses that children have access to, and actively use, specific Social Networking or collaborative working web sites. When this facility is required the children concerned will be added to a specific filtering group which allows access to the named site only, parental agreement will be required before this facility is allowed. It is important that children' full names are not used when accessing blogging sites.

9. Videoconferencing Users

- Children must ask permission from the supervising member of staff before making or answering a videoconference call
- Videoconferencing must be supervised appropriately for the children' age. Parents and carers must agree for their children to take part in videoconferences at least in the annual return
- Responsibility for the use of the videoconferencing equipment outside school needs to be established using a risk assessment for the users
- Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems
- Unique log on and password details for access to JANET / UKERNA videoconferencing services should only be issued to members of staff and kept secure (if you are using the National Education Network)
- Where it might be beneficial for a student or group of children to conference without adult supervision the ICT Services Manager / Network Manager must first give permission

10. Mobile Phones

10.1 Children

Children's mobile phones are not permitted at school. The sending of abusive or inappropriate text messages is forbidden and may be illegal. The inclusion of inappropriate language or images within text messages is difficult for staff to detect. Children will be reminded that such use is both inappropriate and conflicts with school policy. Abusive messages will be dealt with under the school Anti-Bullying Policy; this includes 'videoing' of incidents such as happy slapping etc.

10.2 Staff

Staff will be issued with a school phone where contact with children/parents is required or the school's communication technology, e.g. teachers 2 parents, call parents etc. will be used. If contact with children is necessary staff must use school owned equipment.

11. Handheld Radio Use

When using unencrypted voice radio, the radio must be used within the terms of the Ofcom license and in accordance with relevant school policies. When a secure confidential conversation is required the school mobile or fixed phone network should be used.

12. Security

As more data is available electronically, and in line with our duty under the Data Protection Act (DPA) and General Data Protection Regulation (GDPR), we will take all reasonable steps to protect personal data. A school username and password are required to access school resources and permissions are set so that users can only view areas and documents appropriate to them. Within school unauthorised access to the school's electronic systems would fall under the Computer Misuse Act and will be reported to the police.

Personal data taken off the school site must be protected by encryption. Memory devices are available via the ICT support team on request. Staff should also give careful consideration to the security of laptops which may contain data covered by the Data Protection Act and General Data Protection Regulation. ICT support can advise on the installation of suitable software and this software will be installed on school provided equipment.

Staff should login securely via remote desktop connection or use secure cloud storage, e.g. google drive, when accessing personal data off-site. Where this is not possible all personal data should be protected via encryption.

The disposal of computer equipment which contains non-volatile memory will be managed so that no school data is retained within the devise on disposal.

13. The ICT Use Code of Practice

The school has developed a set of guidelines for computer network use by children and staff. These will be made available to children and kept under constant review by the Headteacher advised by the ICT Services Manager/Network Manager. All members of staff are responsible for explaining the rules and their implications. All members of staff need to be aware of possible misuses and their E-Safety responsibilities towards children.

14. Filtering and Monitoring

The school uses regularly updated and dedicated systems to filter internet content and monitor all student user activity on the network. E-mail messages are monitored and all suspicious items are copied to designated staff.

It is important that all staff maintain high levels of awareness in relation to internet use and proactively monitor student E-Safety, eyes and ears cannot be replaced by electronic systems.

15. Monitoring our Systems

The ICT Support Team will monitor the effectiveness of the systems and practices in place in conjunction with the Headteacher and will recommend to the Leadership Team any changes required to keep pace with evolving technology or use.

16. Cyber-Bullying

Cyber bullying is a form of harassment using information and communications technology (ICT), particularly; mobile phones, social media and internet, with the purpose of trying to deliberately upset and intimidate someone else. It is a "method" rather than a "type" of bullying and includes bullying via text message, instant messenger services, social network sites, email, images and videos posted on the internet or spread by mobile phone.

16.1 Children, Parents and Carers

Parents and carers need to be aware that most children have been involved in cyberbullying in some way, either as a victim, perpetrator, or bystander. By its very nature, cyberbullying tends to involve a number of online bystanders and can quickly spiral out of control. Children and young people who bully others online do not need to be physically stronger and their methods can often be hidden and subtle.
If children or parents/carers of children believe they are being bullied online, they should report this to their Tutor/Head of Year who will follow investigate the incident and use sanctions set out in the behaviour policy to deal with any perpetrators. Where possible, screenshots and evidence of any online activity should be recorded.

16.2 Staff

The school is committed to protecting staff against cyber-bullying and online harassment and take the complaints of staff members as seriously as the complaints of children and parents. Any member of staff who believes they are being bullied or harassed online should report this to the senior leadership team at the school who will investigate the incident. Where possible, screenshots and evidence of any online activity should be recorded.

17. Managing Transgressions

Staff issues will be dealt with by the Headteacher through the normal processes.

Child issues will be dealt with through the school's behaviour policy.

A list of children who have Walled Garden, Restricted or Very Restricted Access will be maintained and this list will give an end (or review) date for the end of a restriction and detail the type of restriction.

Appendix 1: ICT Code of Practice

Children granted access to the internet, including e-mail, will abide by this Code of Practice.

These rules help us to be fair to others and keep everyone safe.

- **I will ask an adult for permission before using the Internet.**
- **The messages I send will be polite and sensible.**
- **I understand that I must never give my home address or phone number, or arrange to meet someone over the internet.**
- **I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.**
- **If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.**
- **I should feel safe and enjoy being on the internet**
- **I should be able to easily search the internet for information**

Student and Parent/Carer Consent

While it is the schools firm intention that access to the internet will be granted to children solely in order to further the teaching objectives of the school, children may have the ability to access other materials as well. The School cannot control the information that may be found on the internet. The information that children may be able to access through the internet may include material that is illegal, defamatory, inaccurate or in some other way objectionable.

Therefore, no student will be granted access to the internet without both student and parent/carer signing the consent forms attached to this Code of Practice.

The parental consent form allows parents/carers to confirm that their child may or may not have access to the internet.

The student consent form confirms that the student has read and agrees to abide by the Code of Practice.

Access and Training

Once signed parental and child consent forms have been received the Network Manager is responsible for granting internet and e-mail access on the School's computer network.

Each student will receive a unique network username and password which should not be divulged to anyone else. A master list of usernames shall be maintained by the ICT support department for the duration of the student's stay at the school.

If a student forgets their network username or password**,** they must request re-issue via their teacher, who will pass the request onto the ICT Services Manager/Network Manager on their behalf.

Note: *Passwords cannot be 'reissued': they will be deleted and a new password will be set up.*

Training and advice on the practicalities and safe use of the internet and e-mail will take place as part of the curriculum and through assemblies.

Withdrawing Access

Internet use during lessons is monitored by the supervising member of staff. All network use/content is logged by the system and anything suspicious will be reported to the ICT Services Manager / Network Manager.

Any child found to have broken or disregarded the Code of Practice may have their internet and/or e-mail access suspended or withdrawn at the discretion of the Headteacher.

The child and parent/carer shall be notified in writing of the withdrawal and reasons for this.

If a child needs network access to complete school work, supervised access may be granted by negotiation with the teacher concerned and the ICT Services Manager / Network Manager.

Access shall be removed from the system by the ICT Services Manager/Network Manager when a child permanently leaves the school and their User Name deleted from the master list.

Monitoring and Review

Implementation and breaches of this policy shall be monitored by the Headteacher and reported to the Governing Body to inform review.

Associated Policies

Data Protection Policy (GDPR), Website Policy, Social Media Policy.

Appendix 2: Internet Access Student Consent Form

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- **I will ask an adult for permission before using the Internet.**

- **The messages I send will be polite and sensible.**
- **I understand that I must never give my home address or phone number, or arrange to meet someone over the internet.**
- **I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.**
- **If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.**
- **I should feel safe and enjoy being on the internet**
- **I should be able to easily search the internet for information**

Signed:

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

E-Safety Agreement

Parent / guardian name: _____

Pupil name: _____

Pupil's class: _____

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, school e-mail and other ICT facilities at school.

- I know that my child has agreed that they will keep to the school's rules for responsible ICT use, outlined in the ICT Code of Conduct.

- I also understand that my child may be informed, if the rules have to be changed during the year. I know that the latest copy of the Online Safety Policy is available on the website or from the school office.

- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

- I understand that the school can check my child's computer files, and the Internet sites they visit.

- I also know that the school will contact me if there are concerns about my child's e-safety or e-behaviour.

- I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent's signature:

Date: _____ / _____ / ____

Appendix 3: Staff Code of Conduct for ICT

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information and communication systems equipment staff are asked to sign this code of conduct.

Members of staff must read and understand the school's ICT / E-Safety policy prior to signing.

I understand that the school ICT equipment and systems are the property of the school whether used on or off the premises. I understand that it is a disciplinary offence to use any school ICT system or equipment for any purpose not permitted by the school.

I will only use the approved, secure email system(s) for any school business.

I appreciate that ICT equipment includes personal ICT devices with the permission of the Headteacher if used for school business. I understand that school information systems and equipment may not be used for private purposes without permission from the Headteacher.

I understand that my use of school information systems, internet and e-mail is monitored and recorded to ensure policy compliance. I will respect system security and I will not disclose or share any password or security information to anyone other than an authorised system manager.

I will not access, try to gain access or distribute any information outside of any restrictions set for my role in the school.

I will not install any software or hardware without permission. I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding the inappropriate use of ICT systems or equipment to the ICT Services Manager / Network Manager, Headteacher or the Designated Child Protection Coordinator.

I will ensure that all electronic communications that I make are compatible with my professional role.

The school may exercise its right to monitor the use of the school's information systems and internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed……**Date**……

Print Name…….