Policy Document

Area: e-Safety

Date written	October 2019
Reviewed by	Amanda Sheppard
Approved by Headteacher	
Approved by Governors	
Review date	October 2020
Review Cycle	Annual

Contents

Introduction

Highfield School is a special school, which provides an appropriate education for pupils aged 11-19 with severe learning difficulties, autism and complex needs. ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.
Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

> Websites • Apps • Email, Instant Messaging and chat rooms • Social Media, including Instagram, Facebook and Twitter • Mobile/ Smart phones with text, video and/ or web functionality • Other mobile devices including tablets and gaming devices • Online Games • Learning Platforms and Virtual Learning Environments • Blogs and Wikis • Podcasting • Video sharing • Downloading • On demand TV and video, movies and radio / Smart TVs.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases). At Highfield School we understand the responsibility to educate our pupils and staff on e-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring

Authorised ICT staff (MINT) may inspect any ICT equipment owned or leased by the school at any time without prior notice. ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime. ICT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account. All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. Please note that personal

communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Training

Annual training should be given to all staff in regard to reporting and recording any concerns and breaches of the acceptable use agreement, e-safety rules and code of conduct. Parents and carers should be informed about appropriate ways to keep their child safe on the internet through tips and guidance on the school website, social media and by information sheets sent home. If there is a concern about their child's use of the internet this should be discussed directly with the parents/carers by phone on in a meeting.

Safeguarding

School have a duty of care towards students and concerns may also be passed on to other relevant professionals. (Social Workers etc…)

Person in school with responsibility for safeguarding:
Rebecca Thompson (Senior DSL)
Person in school with deputy responsibility for safeguarding:
Tracy Marsh (Deputy DSL)
Key Stage DSL
KS5
Amanda Sheppard (Assistant Head Teacher)
Emma Kitchener (Parent Support Advisor)
KS4
Judith Hickey (Assistant Head Teacher)
Lynne Catchpole (Parent Support Advisor)
KS3
Nicola Hirst (Assistant Head Teacher)
Kirsty Barr (Parent Support Advisor)

Writing the e-safety policy

- The e-Safety Policy relates to other policies including those for ICT, anti-bullying and for child protection.
- The school's e-Safety Coordinator is the Assistant Headteacher, who is also a DSL.
- Our e-Safety Policy has been written by the school with regard to Wakefield Council Policies, BECTA, Child Exploitation and Online Protection Centre (CEOP) and DfE guidance.

Highfield School's E-Safety Policy

Internet Use for Children and Young People with SEN

Children with SEN are potentially more vulnerable and more at risk than others when using ICT:

- Those children with ASD may make literal interpretations of content which will affect how they respond.
- They may not understand some of the terminology used.
- Those with more complex needs do not always understand the concept of friendship and therefore trust everyone implicitly. They do not know how to make judgements about what information is safe to share. This leads to confusion about why you should not trust others on the internet.
- Some children may be vulnerable to being bullied through the internet, or not recognize they are being bullied.
- They may not appreciate how their own online behaviour may be seen by someone else as bullying.

Teaching and Learning

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. It is also part of the statutory curriculum and a necessary tool for staff and pupils. Highfield School ensures that:

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the needs of our pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet.
- Parents will be supported by:
    - Information on the safe use of the internet for their families where applicable
    - A link to useful resources on our school website

Internet

Pupils are taught how to evaluate Internet content

- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught how to report unpleasant Internet content to their class teacher, parent, carer

Information system security

- School ICT systems, capacity and security are reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority

E-mail

- Pupils are not given their own e-mail accounts on the school system, but where appropriate an approved email address for their use will be set up for curriculum purposes that is always monitored by the class staff.
- In an email communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers for the use of photographs on the website is requested as part of the annual data collection process.

Social networking and personal publishing

- The school will block/filter access to social networking sites using Wakefield Council recommended filtering software.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for our pupils.

Managing filtering

- The school will work with the Local Authority via an SLA to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Headteacher.
- The ICT Advisor will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
-

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

The use of mobile phones

- Personal mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate messages is forbidden either by text, Bluetooth or any other means.
- Personal phones MUST NOT be used to take photographs of pupils.
- There are mobile phones for work use only. These are vital points of contact for Safeguarding for key staff within the school. Acceptable Usage should always be followed for all members of staff who have access to a work phone. The use of these phones is monitored at all times through software.
- Staff will be issued with a school phone where contact with pupils is required or where mobile phones are used to capture photographs of pupils on educational visits if required.

Games machines

- Games machines, including the Sony PlayStation, Microsoft X box, Nintendo Wii and others have Internet access which includes filtering.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access

- All staff, including those not directly employed by us but working in school, must read and sign the 'Internet Safety and Access Policy, before using any school ICT resource. (Appendix 1)

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wakefield Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the Headteacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
-

Community use of the Internet

The school will liaise with the Children's Centre and other local organisations to establish a common approach to e-safety.

Introducing the e-safety policy to pupils

- E-safety rules, in a format appropriate for our pupils, will be posted in classrooms and discussed with pupils as part of their learning, where appropriate.
- Pupils will be informed that network and Internet use is monitored.
- E Safety training will be embedded within the ICT teaching and learning document and the Personal, Social and Health Education (PSHCE) curriculum.

Social Networking

Staff are made aware that their use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.
Children/young people and their parents/carers **should not** be accepted as friends and any breach of this policy will result in disciplinary action being taken.

All staff representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

Staff Emails

- Staff should not use personal email accounts to communicate with service users.
- Staff should not use work email accounts for personal purposes.

Staff and the E-Safety policy

- All staff will be made aware of the School e-safety policy and its importance explained.
- A copy of the policy will be available in the staff room.
- A copy of the policy statement, Appendix 2, will be posted in the staff room along with Acceptable Use Appendix 1 that staff will also sign each year and be added to their HR file record.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Internet Safety Help Websites for staff

- All internet safety matters in school or any internet safety matter that could have a direct effect on children within the school should be reported using the child protection policy. However further help and advice is available below from these organisations:
- If staff have concerns around internet safety they can visit or contact UK Safer Internet Centre.
  Visit website: https://www.saferinternet.org.uk/professionals-online-safety-helpline
  Email: helpline@saferinternet.org.uk
  Telephone: 0344 381 4772
- For online grooming, or serious concerns about a person's actions online contact National Crime Agency https://ceop.police.uk/safety-centre/
- You can anonymously report child sexual abuse content, criminally obscene adult content and non-photographic child sexual abuse images through the Internet Watch Foundation https://www.iwf.org.uk/
- To talk about internet safety with children http://www.childnet.com/

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus information sheets and on the school Web site.

Appendix 1

Acceptable Use for Employees

- All members of staff are responsible for explaining the rules and their implementations.
- All members of staff need to be aware of possible misuses of online access and their responsibilities towards pupils. This will be updated with regular training for school staff every 2 years and new staff will be given the training on entry to the school.
- The computer system is owned by the school and may be used by students to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties, the pupils, the staff and the school. This will be signed every year by all staff and a version given to visitors on entry to the school.
- The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited and email sent or received.
- Staff, including those not directly employed by the school, requesting Internet access should sign a copy of this Acceptable Use Statement and return it to the School All Internet activity should be appropriate to staff professional activity or the student's education.
- Access should only be made via the authorised accounts and passwords, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is excluded.
- Users are responsible for all email sent and for contacts made that may result in email being reserved.
- Use for personal financial gain, political purposes or advertising is excluded.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is excluded.
- As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is excluded.
- Violation of the above code of conduct will result in a temporary or permanent ban on Internet use.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour
- When applicable, police or local authorities may be involved.

Full name:	**Position in school:**
Signed:	**Date:**
Access granted:	**Date:**

Appendix 2

Policy Statement for School Employees on the Abuse of the Internet

The purpose of this policy is to inform staff that abuse of the Internet in school will be treated extremely seriously with disciplinary action being taken that could lead to dismissal.
The policy should be read together with any school policy on use of the Internet.
Where staff are allowed to use the Internet, it is on the clear understanding that abuse will not occur.
All Internet connections and access through the Council's ICT Network are logged and monitored.

'Abuse' includes:

- Accessing, displaying, downloading or disseminating pornographic or other 'adult' materials
- Posting information that may tend to disparage or harass others on the basis of gender, race, age, disability, religion, sexual orientation, political affiliation or national origin
- Uploading photographs of pupils on to the Internet is forbidden.
- Publishing statements that are defamatory and could bring the school or Local Authority into disrepute
- Publishing information that is false or misleading concerning the school or Local Authority or any other company, organisation or individual that could bring the school or Local Authority into disrepute
- Any activity that breaches the Data Protection Act including publishing confidential or proprietary information of the school or Local Authority, or any of its customers or other business associates, on unsecured Internet sites such as Bulletin Boards or disseminating such information that might compromise its confidentiality
- Unauthorised publishing of information not related to the school or Local Authority
- Knowingly downloading, using, or distributing software or programmes from the Internet without verifying their operational integrity, e.g. the absence of computer viruses and breach of copyright
- Participating in any form of gambling and personal use of the Internet facilities without the specific consent of the Headteacher of the school
- The use of social networking sites in school is not permitted and staff should also be aware that, whilst using these sites outside of school, discussions re school activities/pupils/parents/colleagues is not acceptable and they should note that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 as well as other legislation.

Staff should also note that use of the Internet may be a cost to the school. Authorised personal use should therefore be paid for according to the policy of the school

Appendix 3

E-Safety Social Media Guidance

Appropriate

1. Set your privacy settings for any social networking site.
2. Ensure any technological equipment, (including your mobile phone) is password/ PIN protected.
3. Consider having professional online accounts/ identities if you wish to have online contact with service users, their families and other professionals.
4. Make sure that all publicly available information about you is accurate and appropriate
5. Remember online conversations may be referred to as 'chat' but they are written documents and should always be treated as such.
6. Make sure that you know the consequences of misuse of digital equipment.
7. If you are unsure who can view online material, assume it is public. Remember - once information is online you have relinquished control.
8. Switch off Bluetooth
9. When you receive any new equipment (personal or private) make sure that you know what features it has as standard and take appropriate action to disable/ protect.

Inappropriate

1. Give your personal information to service users -children/ young people, their parents/ carers. This includes mobile phone numbers, social networking accounts, personal website/ blog URLs, online image storage sites, passwords etc.
2. Use your personal mobile phone to communicate with service users. This includes phone calls, texts, emails, social networking sites, etc.
3. Use the internet or web-based communication to send personal messages to children/young people
4. Share your personal details with service users on a social network site
5. Add/allow a service user to join your contacts/friends list on personal social networking profiles.
6. Use your own digital camera/ video for work. This includes integral cameras on mobile phones.
7. Play online games with service users.

This policy statement is subject to revision and staff are advised to consult it regularly

Appendix 4

E-Safety Audit Highfield School

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for the e-safety policy, the ICT Advisor and the Headteacher.

Has the school an e-Safety Policy that complies with Local Authority guidance?		**Y/N**
Date of latest update (at least annual):	October 2019	
The school e-safety policy was agreed by governors on:		
The policy is available for staff at:		
The policy is available for parents/carers at:		
The responsible member of the Senior Leadership Team is:	Amanda Sheppard	
The responsible member of the Governing Body is:		
The Designated Child Protection Coordinator is:		
The e-Safety Coordinator is:	Amanda Sheppard	
Has e-safety training been provided for both pupils and staff?		**Y/N**
Is there a clear procedure for a response to an incident of concern?		**Y/N**
Have e-safety materials from CEOP and Becta been obtained?		**Y/N**
Do all staff sign a Code of Conduct for ICT on appointment?		**Y/N**
Are all pupils aware of the Schools e-Safety Rules?		**Y/N**
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?		**Y/N**
Do parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules?		**Y/N**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored, and individual usage can be traced?		**Y/N**
Has an ICT security audit been initiated by SLT, possibly using external expertise?		**Y/N**
Is personal data collected, stored and used according to the principles of the Data Protection Act?		**Y/N**
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g. KCN, Regional Broadband Consortium, NEN Network)?		**Y/N**
Has the school-level filtering been designed to reflect educational objectives and approved by SLT		**Y/N**