HALFWAYJUNIOR SCHOOL

E-Safety / Online Safety Policy

March 2016
Review: March 2017

Based on a model produced by Sheffield Safeguarding Children Board

"Supporting Each Other to Achieve Success for All"

Rational

The internet and computing technologies are now a part of everyday life within school and at home. They offer many benefits to learning but also pose many risks (including abuse, exploitation and radicalisation). It is the duty of Halfway Junior School to ensure that every child in our care is safe online and knows how to stay safe at home too.

The E-Safety Policy operates in conjunction with other policies including; Safeguarding, Behaviour, Acceptable Use and Curriculum.

Scope of the Policy

This policy applies to all members of the school community (including staff, Governors, pupils, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of school.

- **The Education and Inspections Act 2006** empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying, or other e-safeguarding incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

- **The Education Act 2011** gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any illegal content or material that could be used to bully or harass others. https://www.gov.uk/government/publications/searching-screening-and-confiscation

- **Keeping Children Safe In Education July 2015** This is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Education (Non-Maintained Special Schools) (England) Regulations 2011. Schools must have regard to it when carrying out their duties to safeguard and promote the welfare of children. It should be read alongside statutory guidance **Working Together to Safeguard Children 2015**

- **Counter-Terrorism and Security Act 2015** From 1 July 2015 all schools are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”.

  https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

Monitoring of the policy

Title	**Halfway Junior School E-Safeguarding Policy**
Version	1.0
Date	*1/3/16*
Author	*E-safety Lead (Joanna Kay)*
Approved by the Governing Body on*:*	1/3/16
Monitoring will take place at regular intervals:	*Annual audit and biyearly monitoring*
The Governing Body will receive a report on the implementation of the policy including anonymous details of any e-safeguarding incidents at regular intervals:	*Annually*
The Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safeguarding or incidents that have taken place. The next anticipated review date will be:	*July 2016*
Should serious e-safeguarding incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager* *LA Safeguarding Officer* *Police Commissioner's Office*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys of pupils, parents and staff

Communication of the policy

The senior leadership team will be responsible for ensuring the school community are aware of the existence and contents of the school E-safeguarding policy and the use of any new technology as and when appropriate.

Roles and Responsibilities
We believe that E-safeguarding is the responsibility of the whole school community and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities technology offers in learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Responsibilities of Headteacher and Senior Leaders:
The Headteacher has overall responsibility for safeguarding all members of the school community, though the day to day responsibility for e-safeguarding will be delegated to the E-Safety Lead.

- The Headteacher and senior leadership team are responsible for ensuring that the E-safety Lead and other relevant staff receive suitable training to enable them to carry out their E-safeguarding roles and to train other colleagues when necessary.
- The Headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal E-safeguarding role.
- The Headteacher and senior leadership team will ensure that everyone is aware of procedures to be followed in the event of a serious E-safeguarding incident.
- The Headteacher and senior leadership team receive update reports of any incidents from the E-safeguarding/Safeguarding team.

Responsibilities of the E-Safeguarding Coordinator

- To ensure that the school E-safeguarding policy is current, relevant and reviewed at agreed time intervals.
- To ensure that school Acceptable Use Policies are appropriate for the intended audience.
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.
- To be the first point of contact in school on all E-safeguarding matters.
- To take day-to-day responsibility for E-safeguarding within school and to have a leading role in establishing and reviewing the school E-safeguarding policies and procedures.
- To communicate regularly with school technical staff.
- To communicate regularly with the designated E-safeguarding governor.
- To ensure that all members of staff receive an appropriate level of training in E-safeguarding issues.
- To ensure that E-safeguarding education is embedded across the curriculum.
- To ensure that E-safeguarding is promoted to parents and carers.
- To ensure that an E-safeguarding incident log is kept up to date.

Responsibilities of the Teaching and Support Staff

- To understand, contribute to and promote the school's E-safeguarding policies and guidance.
- To understand and adhere to the school staff Acceptable Use Policy.
- To report any suspected misuse or problem to the E-safeguarding coordinator.
- To develop and maintain an awareness of current E-safeguarding issues and guidance including online exploitation, radicalisation and extremism, bullying, sexting etc.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social media etc.

- To embed E-safeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To understand and be aware of incident-reporting mechanisms within the school.
- To maintain a professional level of conduct in personal use of technology at all times.
- Ensure that sensitive and personal data is kept secure at all times by using only approved and encrypted data storage and by transferring data through secure communication systems.

Responsibilities of Technical Staff

- To understand, contribute to and help promote the school's E-safeguarding policies and guidance.
- To understand and adhere to the school staff Acceptable Use Policy.
- To report any E-safeguarding related issues that come to your attention to the E-safeguarding coordinator.
- To develop and maintain an awareness of current E-safeguarding issues, legislation and guidance relevant to their work such as the Prevent Duty.
- To maintain a professional level of conduct in your personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system.
- To liaise with the senior management team, local authority and other appropriate people and organisations on technical issues.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

Protecting the professional identity of all staff, Governors, work placement students and volunteers

Communication between adults and children by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

When using digital communications, staff, governors and volunteers should:

- only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the school.
- not share any personal information with a child or young person eg should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- not request, or respond to, any personal information from the child, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- Not send or accept a friend request from the child/young person or parent/carers on social networks.

- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- ensure that all communications are transparent and open to scrutiny.
- be careful in their communications with children, parent/carers so as to avoid any possible misinterpretation.
- ensure that if they have a personal social networking profile, details are not shared with children and young people in their care or parents/carers (making every effort to keep personal and professional online lives separate).
- not post information online that could bring the school into disrepute.
- be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Responsibilities of pupils

- To adhere to the school pupil Acceptable Use Policy and to know and understand school policies on the use of digital technologies including digital cameras and any other personal devices.
- To know and understand school policies regarding bullying (inc cyberbullying).
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To discuss E-safeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support the school in promoting E-safeguarding.
- To read, understand and promote the school's E-safeguarding policy.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss E-safeguarding concerns with their children, be aware of what content, websites and Apps they are using, apply appropriate parental controls and ensure they behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology and social media.
- To consult with the school if they have any concerns about their children's use of the internet and digital technology.
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school.

Education

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a safe and responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support to recognise and mitigate risks and build their resilience online.

E-safety will be part of a broad and balanced curriculum and staff will reinforce e-safety messages. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. This will be provided in the following ways:

- A planned e-safety curriculum will be provided as part of Computing and PHSE and other lessons and should be regularly revisited.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies, including promoting Safer Internet Day each year.
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- All use will be monitored and they will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of bullying.
- Pupils will be made aware of where to report, seek advice or help if they experience problems when using the internet and related technologies.

All Staff

It is essential that all staff receive e-safety training and understand their responsibilities as outlined in this policy. Training will be offered as follows:

- All staff will receive regular information and e-safeguarding training.
- All staff will be made aware of individual responsibilities relating to the E-safeguarding of children and know what to do in the event of misuse of technology by any member of the school community.

Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in a safe and responsible way and in promoting the positive use of the internet and social media.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Campaigns eg Safer Internet Day

Use of digital and video images

The development of digital imaging technologies has created significant benefits to teaching and learning, allowing staff and pupils instant use of images that they have uploaded themselves or downloaded from the internet. However, everyone needs to be aware of the potential risks associated with sharing images and with posting digital images on the internet.

- When using digital images, staff will inform and educate pupils about the risks and current law associated with the taking, sharing, use, publication and distribution of images.
- Staff are allowed to take digital / video images to support educational aims or promote celebrations and achievements, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment, including mobile phones, of staff should not be used for such purposes.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Staff will be aware of those pupils where publication of their image may put them at risk.
- Pupils' full names will not be used in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Parents will not publish images of other children online.

Managing ICT systems and access

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible and meets recommended technical requirements.

Filtering internet access

- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will ensure that the filtering system will block extremist content and protect against radicalisation in compliance with the Prevent Duty, Counter-Terrorism and Security Act 2015
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the E-safety Lead. All incidents will be documented.
- The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the Internet Watch Foundation IWF.

Passwords

All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords, e.g.

- Do not write down system passwords.
- Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
- Always use your own personal passwords to access computer based services, never share these with other users.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Never save system-based usernames and passwords within an internet browser.

- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.

Management of Assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The School will:-

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- All access to information systems should be controlled via a suitably complex password.
- All access to the school information management system will be on a need-to-know.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know basis.
- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Incidents of misuse will be treated seriously and will be dealt with through normal behaviour / disciplinary procedures.

Appendices

- Incident Reporting Flow Chart
- Staff and Volunteer ICT Acceptable Use Policy
- Parent E Safety Agreement

Response to an Incident of Concern

Contacts
- Sheffield Safeguarding Advisory Desk 0114 205 3535
- e-Safety Project Manager
- Julia Codman 0114 293 6945
- Sheffield Police 101
- Local Authority Designated Officer (LADO) 2734850

e-Safety Incident Occurs

If a child is at immediate risk
- Inform the Designated Child Protection Coordinator and follow school's child protection procedures
- Seek advice from Safeguarding Advisory Service
- Contact Sheffield Police (999) urgently if there is immediate danger

Illegal Activity of Material found or suspected
- Content
  - Police 999/101
  - Report to Internet Watch Foundation (www.iwf.org.uk)
- Activity
  - Child
    - Contact Safeguarding Advisory Desk for advice
    - Contact Local Authority Designated Officer (LADO)
    - Child protection procedures and / or criminal action
  - Staff
    - Contact Safeguarding Advisory Desk for advice
    - Contact Local Authority Designated Officer (LADO)
    - Staff allegations procedures and / or criminal action

Unsure
- Consult with SSCB Safeguarding Advisory Desk or E-Safety Project Manager

Inappropriate Activity or Material
- Activity
  - Report to E-safety Lead
  - Discuss with Headteacher
    - Child
      - Possible School Actions:
        - Sanctions
        - PHSE/citizenship
        - Restorative Justice
        - Anti Bullying
        - Parental Work
        - School support e.g. counselling, peer mentoring
        - Seek advice from E-Safety Manager
    - Staff
      - Possible School Actions:
        - Staff Training
        - Disciplinary action
        - Involve LADO
        - School support e.g. counselling,
        - Seek advice from E-Safety Manager
- Content

Review Schools e-Safety policies and procedures, record actions in e-Safety Incident log and implement any changes for future

Contact Details

Schools Designated Child Protection Officer: Mrs Carter
School e-Safety Coordinator: Joanna Kay
Safeguarding Children Board e-Safety Manager: 0114 2736945

HALFWAY JUNIOR SCHOOL

"Supporting each other to achieve success for all"

Staff and Volunteer ICT Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, digital cameras, email and social media sites**.**

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password.

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

- I will respect copyright and intellectual property rights.

- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator and/or the e-Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. I will not accept friend requests from parents or children on social media. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the City Council, into disrepute.

- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood the Staff ICT Acceptable Use Policy.

Signed: ……... Print Name: …… Date: ……

Accepted by: ……. Print Name: …….

HALFWAY JUNIOR SCHOOL
"Supporting each other to achieve success for all"

Parent/ Carer E Safety Agreement

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Parents/Carers are asked to sign to show that the e-safety Rules have been understood and agreed.

Parent's Consent for Web Publication of Work and Photographs
I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access
I have read and understood the school e-safety rules and have given permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

As a parent, I support the school policies on E safety and I will ensure that I monitor my child's use of the internet (including social media) outside of school. I will act as a positive role model to my child, by ensuring that I use social media responsibly.

Signed……. Date……..
Please print name……..
Child's Name……

Pupil E Safety Rules

Safe – Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

MEETING – Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

ACCEPTING – Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

RELIABLE – Information you find on the internet may not be true, or someone online may be lying about who they are.

TELL – Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk