POLICY FOR E-SAFEGUARDING

Agreed by Staff	
Agreed by Govenors	
Review date	

1. Introduction

The Darley Centre fully recognises the contribution it can make to protect children and support them in school. The aim of this policy is to safeguard and promote our pupils' safe use of the internet and electronic communication technology. The internet and other technologies have an important role in the learning and teaching processes however, we feel it is important to balance those benefits with an awareness of the potential risks. This policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

The school e-safeguarding policy will operate in conjunction with other policies including Behaviour, Anti-Bullying, Equality, Code of Conduct, Safeguarding, Information Governance and Electronic Acceptable Use with parents/carers.

The school acknowledges e-safety and e-security as important issues for our school community and has made a considered attempt to embed e-safeguarding into our teaching and learning using technology and have considered the wider implications of e-safeguarding beyond classroom practice such as security and data.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safeguarding Policy;
- Secure, filtered broadband;
- The use of e-safety control software monitoring system which monitors and captures inappropriate words or web sites used.

Writing and Reviewing the e-Safeguarding Policy

The e-Safeguarding Policy relates to other policies including those for ICT, anti-bullying and for child protection.

Mike Burnett is the school's e-Safety Co-ordinator.

Our e-Safeguarding Policy has been written by the school, building on the Yorkshire and Humberside grid for learning e-Safeguarding Policy.

2. Our Aims

- To set out the key principles expected of all members of the school community at The Darley Centre with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of The Darley Centre.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

3. Scope of Policy

- This policy applies to the whole school community including Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school and all pupils.
- The senior leadership team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for e-Safeguarding within school will be reflected within this policy.

4. Review and Ownership

- The school has appointed an e-Safeguarding co-ordinator who will be responsible for document ownership, review and updates.
- The e-Safeguarding policy has been written by the school e-Safeguarding Co-ordinator and is current and appropriate for its intended audience and purpose.
- The e-Safeguarding policy is reflected in many other school policies such as the ICT policy, Child Protection policy, Anti-bullying policy, Social Media, Acceptable Use, Code of Conduct and the School Improvement Plan.
- The school e-Safeguarding policy has been agreed by the senior leadership team and approved by governors.
- The e-Safeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- All amendments to the school e-Safeguarding policy will be discussed in detail with all members of teaching staff.

5. Communication of the Policy

- Our senior leadership team and class teachers will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school e-Safeguarding policy and the use of any new technology within school.
- The e-Safeguarding policy will be provided to and discussed with all members of staff and reviewed regularly.
- We endeavour to embed e-Safeguarding messages across the curriculum whenever the internet or related technologies are used.
- The e-Safeguarding policy will be introduced to the pupils at the start of each school year.

6. Roles and Responsibilities

6.1. Responsibilities of the school community

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 that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

- The senior leadership team
- The e-Safeguarding Co-ordinator
- Teachers and support staff

- ICT technician and technical staff
- Pupils
- Parents and carers
- Governing body

6.2. Responsibilities of the senior leadership team

The Headteacher is ultimately responsible for e-Safeguarding provision including e-Safeguarding for all members of the school community.

The Headteacher and senior leadership team are responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their e-Safeguarding roles and to train other colleagues when necessary.

6.3. Responsibilities of the e-Safeguarding Co-ordinator

- To promote an awareness and commitment to e-Safeguarding throughout the 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 create and maintain e-Safeguarding policies and procedures
- 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 all staff are aware of the procedures that need to be followed in the event of an e-Safeguarding incident
- To ensure that an e-Safeguarding incident log is kept up to date
- To ensure that the school Acceptable Use policies are current and pertinent.

6.4 Responsibilities of teachers and support staff

- To read, understand and help promote the school's e-Safeguarding policies and guidance
- To read, 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
- 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 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 ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of e-Safeguarding issues related to the use of mobile phones, cameras and handheld devices
- To maintain a professional level of conduct in personal use of technology at all times

6.5 Responsibilities of ICT technician/technical staff

- To read, understand, contribute to and help promote the school's e-Safeguarding policies and guidance
- To read, 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

- 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 local authority and other appropriate people and organisations on technical issues
- To document all technical procedures and review them for accuracy at appropriate intervals
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted

6.6 Responsibilities of pupils

- To understand and adhere to the school pupil Acceptable Use Policy
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both 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

6.7 Responsibilities of parents and carers

- To help and support the school in promoting e-Safeguarding
- To read, understand and promote the school pupil Acceptable Use Policy with their children
- 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 discuss e-Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children’s use of technology
- To agree to and sign the school’s emergency contact forms which clearly sets out the use of photographic and video images outside of school
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.
- Parents and carers are asked to read through and sign the home school agreement containing a statement about acceptable use
- Parents and carers are required to give written instruction if they do NOT wish for any images of their child to be used.

6.8 Responsibilities of the governing body

- To read, understand, contribute to and help promote the school’s e-Safeguarding policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To monitor how the school ICT infrastructure provides safe access to the internet
- To monitor how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- To support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school

- To ensure appropriate funding and resources are available for the school to implement its e-Safeguarding strategy.

7. Managing Digital Content

7.1 Using images, video and sound

- Parents or carers will indicate if photos and videos can be taken of their child on the initial admission form.
- Parents and carers may withdraw permission, in writing, at any time.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- Pupils and staff will only use school equipment to create digital images, video and sound.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

7.2 Storage of images

- Any images, videos or sound clips of pupils must be stored on the school server network, school ipads or encrypted memory sticks and never transferred to personally-owned equipment.
- The school may store images of pupils that have left the school following their departure for use in school activities and promotional resources.
- Staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.

8. Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will provide a series of specific e-Safeguarding-related lessons in specific year groups as part of the ICT curriculum / PSHE curriculum.
- We will celebrate and promote e-Safeguarding through whole-school activities, including promoting Safer Internet Day.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign in the home school agreement.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member.

8.1. Staff training

- Our staff receive regular information and training on e-Safeguarding issues in the form of annual updates, staff meetings etc.
- As part of the induction process all new staff receive information and guidance on the e-Safeguarding policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safeguarding and know what to do in the event of misuse of technology by any member of the school community.

9. 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.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- All users will sign an end-user Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.

10. Emerging Technologies

New and emerging technologies are being developed constantly in today's fast-moving digital world. These technologies can be anything from handheld devices to new faster communication mechanisms. Schools should try to always be aware of new and appealing technologies as these can, in many cases, offer the potential to develop new teaching and learning tools. As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an e-Safeguarding point of view. We will regularly amend the e-Safeguarding policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an e-Safeguarding risk.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.
- Emerging technologies can incorporate software and/or hardware products.
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school e-Safeguarding and Acceptable Use policies.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.

The school will audit ICT equipment usage to establish if the e-Safeguarding policy is adequate and that the implementation of the e-Safeguarding policy is appropriate.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- Methods to identify, assess and minimise risks will be reviewed regularly

11. Filtering Internet Access

As all schools will be aware, the internet is a valuable tool for teaching and learning. Unfortunately, not all content that is available on the internet is suitable for schools, so provision has to be made to ensure that a suitable, fit-for-purpose internet filtering solution is deployed.

- The school uses a filtered internet service.
- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- 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-Safeguarding Coordinator. All incidents should be documented.
- The school will regularly review the filtering product for its effectiveness.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

12. Internet Access Authorisations

Schools should allow internet access to staff and pupils on the grounds that it is required for either work-related purposes or for educational need.

- Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate.
- All pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy prior to being granted internet access within school.
- All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy prior to being granted internet access within school.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.

13. Email

Electronic mail (email) is an essential communication mechanism for both staff and pupils in today's digitally-connected world. The use of email can bring significant educational benefits for any school, both for its staff and pupils. However, email use for staff and pupils needs to be thought through and appropriate safety measures put in place.

Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.

- Pupils may only use school-provided email accounts for school purposes.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- It is the responsibility of each account holder to keep the password secure.
- School email accounts should be the only account that is used for school-related business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

13.1 Email usage

- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils and staff will be reminded when using email about the need to send polite and responsible messages.
- Pupils and staff will be reminded about the dangers of revealing personal information within email conversations.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.
- Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- Pupils must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.
- Irrespective of how pupils or staff access their school email (from home or within school), school policies still apply.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- Staff who send emails to parents, are advised to carbon copy (cc) or include the Headteacher, line manager or another suitable member of staff into the email.

14. Mobile Phone Usage in School

In today's digital world, communications and content are available almost anywhere at any time. Gone are the days when mobile phones could only be used for making phone calls. They are now multi-functional, smart devices which can be used for browsing the internet, email, texting, mobile applications, social networking, photography and video. Modern-day smart phones are effectively mobile computers, which are far more powerful and feature-rich devices than the original home computers.

14.1 General issues

- Mobile phones and personally owned devices will not be used in any way during lessons or formal school time.
- Mobile phones and personally owned mobile devices brought in to school by staff are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices. It is advised that they are locked away in desks or the classroom cupboard.
- No images or videos should be taken on mobile phones or personally-owned mobile devices. (See photography policy)

14.2 Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Mobile Phones and personally owned devices will be switched off or switched to 'silent' mode during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then they may use their own devices and hide (**by inputting 141**) their own mobile numbers for confidentiality purposes.

15. Data Protection and Information Security

Schools should have a current registration for data protection. As a commitment to this registration, they will be complying with the Data Protection Act 1998, with guidance from their local authority. Schools hold lots of information and data on pupils, families and on staff. The amount of information which schools hold is increasing all the time and, while this data can be very useful in improving the service which a school provides, the school has a duty of care for how it handles and controls access to the sensitive and personal information and data which it holds.

The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

The Data Protection Act 1998 establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to have respect for the privacy of their personal details. The legislation itself is complex and, in places, hard to understand. However, it is underpinned by a set of nine straightforward, common-sense principles. If we make sure we handle personal data in accordance with the spirit of those principles, then we will go a long way towards ensuring that you comply with the letter of the law.

- Data should be processed fairly and lawfully
- Data should be obtained only for one or more specified and lawful purposes
- Personal data held shall be adequate, relevant and not excessive
- Data should be accurate and up to date
- Data should be held no longer than for the purpose it was originally collected
- Data should be processed in accordance with individual's rights
- Data should be secured accordingly
- Appropriate technical and organisational measures should be taken to secure all data held
- Data should be transferred only to other countries with suitable or equivalent security measures.

View the Information Governance policies for further information.

15.1 Senior Information Risk Owner (SIRO) - Headteacher

The Senior Information Risk Owner is a senior member of staff who is familiar with information risks and the organisation's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities.

- They own the information risk policy and risk assessment
- They appoint the information asset owners (IAOs)
- They act as an advocate for information risk management

The Office of Public Sector Information has produced a publication 'Managing Information Risk' to support SIROs in their role.

15.2 Information Asset Owner (IAO) – School Office Manager

The role of the IAO is to understand:

- What information is held, and for what purposes
- How information will be amended or added to over time
- Who has access to the data and why
- How information is retained and disposed off

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. Although a school will appoint these key roles, the handling of secured data is everyone's responsibility, whether they are an employee, volunteer, technical support or third party provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even provoke legal action.

16. Management of Assets

All schools will have both software and hardware assets for both educational and administrative purposes. All equipment and software comes at a cost to the school and should therefore be controlled and documented appropriately.

By maintaining valid inventories, schools should be in a position to extract full value from their purchases as educational activities can be based and planned around the assets they hold. It should also not be overlooked that recording information on all equipment can also assist in hardware replacement programmes and software upgrades, as spending can be planned against asset age and specification.

Schools should also be aware that any old hardware such as laptops, PCs, servers and removable media needs to be formatted prior to disposal (or through a third party) to ensure no sensitive or personal data remains on old hardware.

- Details of all school owned hardware will be recorded in an electronic hardware inventory.
- All redundant ICT equipment will be disposed of through an authorised agency (recommended by the LA). 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

Richard Martin
Senior Teacher
December 2018

Agreed by staff:
Approved by Governors:
Review Date: December 2019