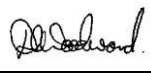
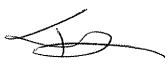
Bradford Central PRU

eSafeguarding Policy

Policy agreed by Staff on:	March 2017
Ratified by full Management Committee:	March 2017
Review Date:	Spring 2018
Agreed Frequency of Review:	Yearly
Allocated Group / Person to Review:	MC can delegate to committee or individual member or HT
Signed by Chair:	
Signed by Headteacher:	

Policy introduction
The eSafeguarding policy has been written to ensure safety measures are in place to protect both pupils and staff working with ICT equipment and related technologies at BCPRU. The policy is to assist PRU staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor pupil standards and practice. Our responsibility is to set high expectations of our pupils using communication technologies and to maintain a consistent approach to eSafeguarding by knowing the content of the policy and the procedures adopted and developed by the PRU.

Scope of policy

- This policy applies to the whole BCPRU community including the Senior Leadership Team (SLT), the Management Committee and all staff employed directly or indirectly by the PRU and all pupils.
- The Management Committee and the SLT of BCPRU will ensure that any relevant or new legislation, which may impact upon the provision for eSafeguarding within the PRU, will be reflected within this policy.
- The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils or pupils when they are off the PRU site. This is pertinent to incidents of cyberbullying, or other eSafeguarding related incidents covered by this policy, which may take place out of the PRU, but is linked to membership of the PRU.
- The PRU will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate eSafeguarding behaviour that takes place out of the PRU.

Review and Ownership

- The BCPRU eSafeguarding policy has been agreed by the Senior Leadership Team (SLT) and approved by the Management Committee.
- The BCPRU eSafeguarding policy will be reviewed annually or when any significant changes occur with regards to the technologies in use within the PRU.
- The PRUs have appointed a member of the Management Committee to take lead responsibility for Safeguarding. This will include eSafeguarding.
- Amendments to the BCPRU eSafeguarding policy will be discussed in detail with all members of teaching staff.

We believe that eSafeguarding is the responsibility of the whole BCPRU 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 Responsibility of the Senior Leadership Team

- The Headteacher is ultimately responsible for safeguarding provision (including eSafeguarding) for all members of the PRU community, though the day-to-day responsibility for eSafeguarding will be delegated to the Heads of Centre (HOC).
- The Headteacher is responsible for ensuring that the HOCs and other relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.
- The Headteacher will have regular contact with the named members of the Management Committee for safeguarding.
- The Headteacher and SLT should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.
- The HOCs will give updates and information relating to eSafeguarding incidents to the Headteacher on a regular basis.
- The SLT will promote an awareness and commitment to eSafeguarding throughout the PRU.
- The HOCs will be the first point of contact at PRU on all eSafeguarding matters.

- The HOCs will communicate regularly with the Business Manager relating to ICT and eSafeguarding.
- The SLT will maintain eSafeguarding policies and procedures.
- The SLT will ensure that eSafeguarding education is embedded across the curriculum.
- The SLT will ensure that eSafeguarding is promoted to parents and carers.
- The SLT will ensure that all staff are aware of the procedures that need to be followed in the event of an eSafeguarding incident.
- The SLT will understand the issues surrounding the sharing of personal or sensitive information.

Responsibility of Teachers and Support Staff

- To read, understand and help promote the PRU's eSafeguarding policies and guidance.
- To read, understand and adhere to the PRU staff Acceptable Use Agreement.
- To report any suspected misuse or problem to the HOC.
- To develop and maintain an awareness of current eSafeguarding 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 PRU based systems, **NEVER** through personal mechanisms, e.g. email, text, mobile phones, social networking etc.
- To embed eSafeguarding 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 methods.
- To be aware of eSafeguarding issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms that exist within the PRU.
- To maintain a professional level of conduct in personal use of technology at all times.

Responsibility of The Business Manager and Administrators

- To read, understand, contribute to and help promote the PRU's eSafeguarding policies and guidance.
- To read, understand and adhere to the PRU staff Acceptable Use Agreement.
- To report any eSafeguarding related issues that come to your attention to the HOC.
- To develop and maintain an awareness of current eSafeguarding 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 PRU in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the PRU 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 PRU 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 PRU-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within PRU.
- 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 PRU-owned software assets is restricted.

Responsibility of Pupils

- Pupils will understand and adhere to the PRU Pupil Acceptable Use Agreement.
- To help and support the PRU in the creation of eSafeguarding policies and practices and to adhere to any policies and practices the PRU creates.
- Pupils will be expected to understand PRU policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand PRU rules relating to bullying and cyberbullying.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in the PRU and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in the PRU and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to understand the incident-reporting mechanisms that exists within the PRU.
- To discuss eSafeguarding issues with family and friends in an open and honest way.

Responsibility of Parents and Carers

- To help and support the PRU in promoting eSafeguarding.
- To read, understand and promote the Pupil Acceptable Use Agreement 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 the PRU 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 eSafeguarding 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 PRU if they have any concerns about their children's use of technology.
- To agree and sign the consent form stating that their child will follow acceptable ICT use.
- To agree and sign the consent form allowing for permission for photographic and video images of their child to be taken and published/displayed in public.

Responsibility of the Management Committee

- To read, understand, contribute to and help promote BCPRU eSafeguarding policies and guidance.
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- To develop an overview of how the BCPRU ICT infrastructure provides safe access to the internet.
- To develop an overview of how the BCPRU encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of the PRU.
- To support the work of the PRU in promoting and ensuring safe and responsible use of technology in and out of the PRU, including encouraging parents to become engaged in eSafeguarding activities.
- To ensure appropriate funding and resources are available for the PRU to implement its eSafeguarding strategy.
- To develop an overview and understanding as the body corporate in relation to their responsibilities regarding the PRUs Data Protection commitments.

Responsibility of the Named Persons

- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyberbullying and the use of social media for this purpose.

Responsibilities of other external groups

- The PRU will liaise with local organisations to establish a common approach to eSafeguarding and the safe use of technologies.
- The PRU will be sensitive and show empathy to internet-related issues experienced by pupils out of PRU, e.g. social networking sites, and offer appropriate advice where appropriate.
- Any external organisations will sign an Acceptable Use Agreement prior to using any equipment or the internet within the PRU.
- The PRUs will provide an Acceptable Use Agreement for any guest who needs to access the PRU computer system or internet on PRU grounds. (Parent helpers, trainee teachers, work experience pupils etc.).

Managing Digital Content

- Before photographs of pupils can be published, the consent form allowing for permission for photographic and video images of their child to be taken and published/displayed in public must be signed by the pupil and parent.
- All staff are aware of the process involved with publishing images over different mechanisms.
- Parents and carers may withdraw permission, in writing, at any time.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at the PRU and at home.
- Pupils and staff will only use PRU equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the Headteacher provided that any media is transferred solely to a PRU device and deleted from any personal devices. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved.
- Parents may take photographs at PRU 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 - unless appropriate security settings are enabled and set to maximum.
- When searching for images, video or sound clips, staff will be taught about copyright and acknowledging ownership.
- When searching for images, video or sound clips staff will ensure that pupil's usage is monitored for copyright purposes.

Storage of images

- Any images, videos or sound clips of pupils must be stored on the PRU network and never transferred to personally-owned equipment. The PRUs will store images of pupils that have left the PRU for a number of 5 years following their departure for use in PRU activities and promotional resources.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.
- The Business Manager has the responsibility of deleting the images when they are no longer required.

Teaching and Learning

- We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our PRU community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in the PRU 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 discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- 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.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- Pupils will be taught about the impact of bullying and cyberbullying and know how to seek help if they are affected by any form of online bullying.
- 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, or an organisation such as Childline or the Child Protection On-line Protection Centre (CEOP) report abuse button.

Staff training

- Our staff receive regular information and training on eSafeguarding issues in the form of annual updates, termly where applicable.
- As part of the induction process all new staff receive information and guidance on the eSafeguarding policy and the PRU's Acceptable Use Agreements.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the PRU community.
- All staff will be encouraged to incorporate eSafeguarding activities and awareness within their curriculum areas.

Managing ICT systems and access

- The PRUs 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.
- Members of staff will access the internet using an individual username and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their username and password. They will abide by the PRU Acceptable Use Agreement at all times.

Passwords

- A secure and robust username and password convention exists for all system access. (Email, network access, PRU management information system).
- All information systems require staff to change their password at first log on.
- Staff should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.

- Staff should change their passwords whenever there is any indication of possible system or password compromise.
- All staff have a responsibility for the security of their username and password. Staff must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Staff are expected to comply with the following password rules.
- 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.

New technologies

- We will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an eSafeguarding point of view. We will regularly amend the eSafeguarding policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an eSafeguarding risk.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in PRU is allowed.
- The PRU will audit ICT equipment usage to establish if the eSafeguarding policy is adequate and that the implementation of the eSafeguarding 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.

Mobile phones

- There are clear rules which all pupils are aware of around the use of phones and devices and they fully understand they should be switched off and handed in to a responsible adult on entry to the classroom.
- Phones that are handed in will be stored securely and returned to the pupil at the end of the PRU day.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a PRU phone. Parents are advised to contact the PRU reception if the need arises.

Staff use of mobile 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.
- Certain identified staff will be issued with a PRU phone where contact with pupils, parents or carers is required.
- Mobile phones and personally-owned devices will be stored securely with personal belongings within the PRU.
- 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.

Filtering internet access

- The PRU's internet provision will include filtering appropriate to the age and maturity of pupils.
- The PRU will always be proactive regarding the nature of content which can be viewed through the PRU's internet provision.

- The PRU 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 Agreement and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to the HOC. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the HOC. The PRU will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the Internet Watch Foundation (IWF).
- The PRU will regularly review the filtering product for its effectiveness.
- The PRU filtering system will block all sites on the IWF list and this will be updated daily.
- Any amendments to the PRU filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Pupils will be taught to assess content as their internet usage skills develop.
- 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-PRU requirement across the curriculum.

Internet access authorisations

- Parents will be encouraged to read the PRU Acceptable Use Agreement for pupil access and discuss it with their children.
- All pupils will have the appropriate awareness training and where possible, sign the pupil Acceptable Use Agreement prior to being granted internet access within the PRU.
- All staff will have the appropriate awareness training and sign the staff Acceptable Use Agreement prior to being granted internet access within the PRU.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- The PRU will maintain a current record of all staff and pupils who have been granted access to the PRUs' internet provision.
- Any visitor who requires internet access will be asked to read and sign the Acceptable Use Agreement.
- When considering internet access for vulnerable members of the PRU community the PRUs will make decisions based on local knowledge.
- All pupils will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

Email

- Staff should only use approved email accounts allocated to them by the PRU and should be aware that any use of the PRU email system will be monitored and checked.
- Where possible access to personal email accounts should be restricted to non-contact time and should be kept to a minimum.
- Staff should not use personal email accounts during PRU hours or for professional purposes, especially to exchange any PRU-related information or documents.
- Access, in the PRU, to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and productivity and will be restricted in line with the PRU eSafeguarding and Acceptable Use Agreements.
- The PRU gives all staff their own email account to use for all PRU business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.
- PRU email accounts should be the only account that is used for PRU-related business.
- Staff will only use official PRU-provided email accounts to communicate with pupils and parents and carers, as approved by the SLT.

- Under no circumstances should staff contact pupils, parents or conduct any PRU business using personal email addresses.
- Irrespective of how staff access their PRU email (from home or within the PRU), PRU policies still apply.
- Emails sent to external organisations should be written carefully and, where necessary, authorised before sending to protect the member of staff sending the email.
- Chain messages will not be permitted or forwarded on to other PRU-owned email addresses.
- The PRU requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the PRU'.
- All emails should be written and checked carefully before sending, in the same way as a letter written on PRU-headed paper.
- Staff who send emails to external organisations, parents or pupils, are advised to carbon copy (cc) their line manager or another suitable member of staff into the email.
- All emails that are no longer required or of any value should be deleted.
- Email accounts should be checked regularly for new correspondence.
- When away for extended periods, 'out-of-office' notification should be activated so that colleagues are aware that you are not currently available.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies need to be controlled and never communicated through the use of a personal account
- Staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- All email and email attachments will be scanned for malicious content.
- Staff should never open attachments from an untrusted source but should consult the Business Manager.
- Communication between staff and pupils or members of the wider PRU community should be professional and related to PRU matters only.
- Any inappropriate use of the PRU email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately.
- All email users within PRU should report any inappropriate or offensive emails through the incident-reporting mechanism within the PRU.
- Pupils must immediately tell the HOC if they receive any inappropriate or offensive email.
- Pupils may only use PRU-approved accounts on the PRU 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.
- Pupils must not reveal personal details of themselves or others in email communications. Pupils should get prior permission from an adult if they arrange to meet with anyone through an email conversation.

Using blogs, wikis, podcasts and other mechanisms to publish content online

- Blogging, podcasting and other publishing of online content by pupils will take place within the PRU learning platform or PRU website.
- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Any public blogs run by staff on behalf of the PRU will be hosted on the learning platform/PRU website/blog and postings should be approved by the HOC before publishing.
- Staff will model safe and responsible behaviour in their creation and publishing of online content within the PRU learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.

- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the PRU where possible.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside PRU.

Use of Social Media

- Staff must not talk about their professional role in any capacity when using personal social media such as Facebook and YouTube or any other online publishing websites.
- Staff and pupils are asked to report any incidents of cyberbullying to the PRU.
- Staff will raise any concerns about pupil use of social media sites with parents/carers this includes the use of any sites that are not age appropriate.
- All staff will receive training on the risks associated with the use of social media either through staff meetings or via the induction process for new starters. Safe and professional behaviour is outlined in the Acceptable Use Agreement.
- Staff must not use social media tools to communicate with current or former pupils under the age of 18.
- Staff will not use any social media tools to communicate with parents unless approved in writing by the Headteacher.
- Procedures for dealing with cyberbullying incidents of staff or pupils involving social media are outlined in the Anti-Bullying Policy.
- Staff are advised to set and maintain profiles on such sites to maximum privacy and to give access to known friends only.

Data protection and information security

- The PRU community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The PRU has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within PRU.
- The PRU has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the PRU will be controlled appropriately through technical and non-technical access controls.
- All computers that are used to access sensitive information should be locked (Ctrl-Alt-Del or equivalent) when unattended.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- Any access to personal and sensitive information should be assessed and granted by the Business Manager.
- All access to the PRU information management system will be on a need-to-know or least privilege basis. All access should be granted through the Business Manager.
- All information on PRU servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/least privilege basis. All access should be granted through the Business Manager.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the PRU.
- All physical information will be stored in controlled access areas.
- Fax machines will be situated within controlled areas of the PRU.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted full disk, and encrypted removable media, remote access over encrypted tunnel.

- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the PRU's information-handling procedures and, for example, not left in cars or insecure locations.

Management of assets

- Details of all PRU-owned hardware will be recorded in a hardware inventory.
- Details of all PRU-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 will be cleared multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The PRU 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.

Special requirements

- We will seek to ensure that all users have access to ICT through the use of a range of specially adapted hardware.