Acceptable and Expected Use of Digital Technologies Policy

2021

Version Control:

Version 1 -   Adapted from Northamptonshire County Council's AUP
               "which schools and other children's services can download and adapt to suit their needs,"
               by TB, 19/10/09.

Version 2* -   Significantly updated to reflect changing technologies, needs, school systems and procedures,
               by AB and JP, February/March 2012*

Version 3* -   Updates/clarifications by JP: May 2015*, January 2017*, May 2017*, October 2017*, May 2018*,
               March 2019*

Version 4* -   Trustwide updates/clarifications by JP: September 2021

1. What is an Acceptable and Expected Use of Digital Technologies Policy?

This policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all digital/online technologies for adults and children within the Trust.

It also states how the Trust will provide support and guidance to pupils, parents/carers and families for the safe and responsible use of these technologies beyond school settings.

2. Why have an AUP?

The use of digital/online technologies as tools to develop learning and understanding has become an integral part of school and home life. It is imperative that there are clear rules, procedures and guidelines to minimise any inherent risks and especially so when children use these technologies.

These risks include:
- Commercial issues with spam, inappropriate email, phishing and cyber attacks
- Viruses which may compromise Trust, Academy and personal security
- Potentially illegal activities such as downloading copyright materials, file-sharing and more serious issues such as the creation and sharing of sexual imagery
- Online content which is upsetting or abusive
- Cyber-bullying and grooming
- Exposure or access to extremist or terrorist materials. Radicalisation.

It is important that staff are clear about appropriate procedures, for example, only contacting children about homework within secure online environments, not by email, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

The Trust acknowledges that whilst it will endeavour to safeguard against all risks it may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure that children are best protected.

It is the duty of our schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Therefore, the active involvement of both children and their parents/carers is vital to the successful use of online technologies. This policy aims to inform how pupils and parents/carers are part of the procedures and how children should be educated to make good judgements about what they see, find and use. The term 'e-Safety' is used to encompass the safe use of all online technologies in order to protect children and adults from known and potential risks.

3. AUP Aims

- To ensure the safeguarding of children within and beyond the school setting by detailing appropriate and acceptable uses of online technologies.
- To outline the roles and responsibilities of everyone.
- To have clarity about procedures following the misuse of any online technologies both within and beyond the school setting.

4. Roles and responsibilities within a Trust Academy:

4.1 Roles: Governors, Principals, Vice Principals and e-Safety Leaders

It is the overall responsibility of the Principal, Vice Principal and e-Safety Leader with the Governors to ensure that there is an overview of e-Safety (as part of the wider remit of Child Protection) across each Academy with specific responsibilities as follows:

- The Principal and Vice Principals are responsible for promoting e-Safety across the curriculum and have an awareness of how this is being developed
- An e-Safety Leader will implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe learning/working environment.
- The Principal will inform the Governors at Curriculum meetings about the progress of the e-Safety curriculum and ensure Governors know how this relates to child protection. At full Governor meetings all Governors will be made aware of any key e-Safety developments.
- The Governors **MUST** ensure Child Protection is covered with an awareness of e-Safety and be clear how it is being addressed within each Academy. It is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.
- An e-Safety Governor will, where necessary, challenge the e-Safety Leader about this AUP having appropriate strategies to clearly define the roles and responsibilities for the management, implementation and safe use of online technologies.
- These parties will jointly ensure that any misuse or incident is dealt with according to policy and appropriate action is taken, to extremes such as suspending a member of staff or involving the Police. See appendices for procedures on misuse.

4.2 Roles: e-Safety Leader
It is the role of the designated e-Safety Leader to:
- Liaise with the PSHE, Child Protection and Computing/ICT leads so that all policies and procedures are up to date to take account of any emerging issues and technologies.
- Provide up-to-date information for all staff to teach and manage e-Safety effectively.
- Involve parents/carers so they feel informed and know where to go for advice.
- Ensure there is appropriate and up-to-date anti-virus and anti-spyware software on all susceptible devices and that this is reviewed and updated on a regular basis.
- Ensure that filtering is set to the correct level for staff and children at the initial set up of all devices and within any online environments.
- Develop and maintain staff awareness of the nature and likelihood of phishing and cyber-attacks. Train staff to be alert to the typical signs of such attacks and to know how to best protect themselves, the Academies and the wider Trust from these.
- Have an overview of all Academy digital/online technology usage –
  it is the class teacher's responsibility to monitor such usage by the children in their class.
- Keep a log of incidents for analysis to help inform future development and safeguarding.
- Report issues and update the Principal on a regular basis.
  This will be reported, as necessary, in the Governors' Operational Committees.
- Ensure that the AUP is reviewed annually.

4.3 Roles: Staff or adults in the Trust
It is the responsibility of all staff/adults within an Academy to:
- Ensure that they know who the Designated Person for Child Protection is so that incidents which involve a child can be reported. Where an allegation is made against a member of staff it should be reported immediately to the Principal. In the event of an allegation made against the Principal, the Chair of Governors must be informed immediately.
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed immediately.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via digital technologies in the same way as for other non-physical assaults.
- Be up to date with e-Safety knowledge that is appropriate for the age group they work with and embed this throughout the curriculum.
- Be aware of the Prevent (Radicalisation) Agenda and act appropriately upon any concerns.

- Ensure that children and young people are protected and supported in their use of online technologies so that they know how to use them in a safe and responsible manner and know what to do in the event of an incident.
- Monitor pupil's choices of usernames within any online environments.
- Respond promptly if a pupil believes any of their passwords is known by others.
- Keep Academy information confidential and not breach the Data Protection Act.
- Only upload pupil information, as required by specific job roles, to online database-requiring services (for example Seesaw and SIMs) for agreed purposes*, such as monitoring pupil progress and/or enhancing children's learning. *Such service providers must have been approved by the school and vetted by the Data Protection Officer.
- Not disclose security passwords or leave a device unattended when they are logged in.
- Follow security procedures if any data is required to be taken from the school premises.
- Use caution and measures such as installed anti-virus software to prevent the transfer of viruses to the school network from removable media and the internet.
- Be alert to the signs of phishing/cyber-attacks, eg. anything unexpected about the arrival, nature or layout of an email, especially if it invites the recipient to click on a button, follow a link or open an attachment. Such emails should be deleted or further enquiries made.
- Report any accidental 'misuse' or access to inappropriate materials to the e-Safety Leader.
- Appropriately use only devices provided by (or authorised by) the Academy. Any use deemed necessary of personal equipment, should be agreed with, or reported promptly to, the e-Safety Leader, a Vice Principal or the Principal.
- Only use Academy provided USB memory sticks and follow agreed encryption procedures.
- Use devices provided by the Academy when working at home or ensure that any personal devices used for work purposes at home have up-to-date anti-virus and malware protection and are password protected. No Academy personal information (including photographs) should be saved onto any home devices or printed at home.
- Alert the e-Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff and adults – see Appendix 1.

4.4 Roles: Children
Children will be:
- Involved in the review of our Acceptable Use Policy through the school council or other appropriate groups, in line with this policy being reviewed and updated.
- Taught to use digital/online technologies in a safe and responsible manner through Computing/ICT, PSHE and across the curriculum.
- Taught to tell an adult about accessing any inappropriate materials or contacts from someone they do not know or other issues straightaway.

4.5 Roles: Parents/Carers
We want our parents/carers to feel involved and active in the e-safety education of their children. Academies should keep parents informed about potential risks and current best guidance. Parents should know where to go for advice and support, starting with their child's class teacher. It should be clear that this support extends beyond the school day and gates; it is more likely that issues will occur outside of schools rather than within.

5. Appropriate use by staff or adults at the Academy
Staff members who have password protected access to the Trust/Academy networks have this so that they can access, develop and manage appropriate resources for the children they teach and other Trust/Academy work. Staff also have access to a range of peripheral ICT equipment which is similarly resourced/supplied to appropriately deliver the work of the Trust/the Academies.

All staff will be made aware and asked to read/follow this Policy, including a requirement to sign the Acceptable Use Rules for Staff (appendix 1), which makes clear how the Trust's digital/online resources should be used. An abridged version of the Rules will be given to adults who work in the Academy for short periods (appendix 4).

5.1 In the event of inappropriate use by staff or adults at the Academy
If a member of staff is believed to have deliberately misused any of the Academy's digital/online resources in any manner suspected to be inappropriate, a report must be made to the staff member's Principal immediately.

Also see appendix 2 – 'Procedures Following Misuse by Staff' (this includes minor events and accidental misuse and has for a list of actions relating to the scale of the incident).

6. Appropriate use by children
Within the Trust children are taught to use the digital/online technologies in a safe and responsible For example, knowing how to conduct research or write an email to another child.

The downloading of materials, for example music files or photographs needs to be appropriate and 'fit for purpose' eg. based on research for work and be copyright issue free. Children will be taught and encouraged to consider the implications of misusing digital/online technologies such as posting hurtful/inappropriate material online.

In the event that a pupil accidentally accesses upsetting or inappropriate content the child should know appropriate actions to take eg. close the window and report this to an adult immediately.

Where a child or young person feels unable to disclose any issues or misuses against them to a trusted adult, they should have been made aware of the facilities such as the CEOP Report Abuse button (www.thinkuknow.co.uk) and Childline number (0800 1111) to seek advice and help.

6.1 In the event of inappropriate use by children – 'internal'
Children will be supported if there are any accidental incidents. Should a child be found to have deliberately misused digital/online resources the following consequences will occur:
- The parents/carers of the child will be contacted
- A formal incident record will be made
- Further or serious misuse of the rules may result in a suspension of access to some digital/online resources for a period of time and a letter will be sent to parents/carers (this would include any incident where a child is deemed to have misused technology against another child or adult).
- Depending on the seriousness of the incident other sanctions may be employed.

Also see appendix 3 – 'Procedures Following Pupil Misuse or Incident'

6.2 In the event of inappropriate use by children – 'external'
If the Academy becomes aware of an incident outside of school, it will raise this with any parents/carers involved and offer guidance toward its resolution. In extreme cases some such situations may require the contacting of outside agencies such as the police, or in cases of radicalisation to the Channel Scheme.

In cases of 'youth produced sexual imagery', (a specific definition of 'sexting') the Academy will follow 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'.
All members of staff (including non-teaching) will be trained how to recognise and disclose such incidents and pupils will be given age appropriate e-Safety teaching in this area.

6.3 In the event of concerns of radicalisation
In respect of safeguarding individuals from radicalisation, the Academy follows the Prevent element of the Government's Counter Terrorism Strategy, and where deemed appropriate seeks external support for <u>members of the Academy community</u>* through referrals to the Channel Programme. This programme aims to work with the individual to address their specific vulnerabilities, prevent them becoming further radicalised and possibly entering the criminal justice system because of their actions. It is recognised that radicalisation can occur to an individual from any section of society and is not particular to any racial, ethnic or social group. It is further recognised that in many instances the process of radicalisation is essentially one of grooming by others.
*Any individuals, child or adult, that employed personnel come into contact within the course of their work.

7. The curriculum and tools for learning
7.1 Internet use
Children will be taught how to use online digital technologies safely and responsibly, for researching information, exploring concepts, deepening knowledge and communicating effectively in order to further learning. This will be through both Computing and PSHE lessons and across the curriculum. The following concepts, skills and competencies will be taught by the time pupils leave Year 6:
- internet literacy, including making good judgements about websites
- understanding risks such as viruses and opening mail from a stranger
- knowledge of copyright, plagiarism, file-sharing and downloading illegal content issues
- data privacy awareness – knowing what is and is not safe to upload
- how to access to appropriate guidance, where to go for advice and how to report abuse

These skills and competencies will be taught within the curriculum so that children have the security to explore how online technologies can be used effectively and in a safe and responsible manner. Pupils will know how to deal with any incidents with confidence.

Personal data safety – we will ensure that information uploaded to websites and otherwise placed in the public domain does not include pupil's personal information including their:
- full name
- address, telephone number and DoB

7.2 Contributions to online communities
Staff approval is required before children make contributions to any external online community such as a forum, blog or wiki. Staff, in turn, must gain the approval of the e-Safety Leader before children participate in any externally controlled community including online chatrooms or webcam links.

7.3 Email use
Staff should not communicate with parents directly via their school email address – all such communication should be through each Academy's contact email address. If parents contact staff directly they should not reply. They should forward the email to the official Academy contact email address (or, if potentially contentious, to a Senior Leader) and set up a filter rule to ensure that no further emails are received.
Any replies to parents should be in school working hours (unless directed from a Senior Leader to reply outside of these hours).

7.4 Mobile phones and related technologies
Without the express permission of a staff member pupils use of mobile phones is not allowed in the Academies or on school grounds during the school day, at after-school clubs, on a school trip or residential visit. Pupils may leave mobile phones in the main school office for the day.

Unless directed to do so, and then blocking their number, staff should not use their personal phones to contact parents. Children must not be contacted un this way.

8. Photographs and video
The term 'image' refers to the taking of photographs or video via any camera or other technology.

Academy images of children will not be in any way compromising or inappropriate. If a member of staff is unsure if a photograph is appropriate for publication, they should seek guidance from the e-Safety Leader, a Vice Principal or the Principal.

Images should only reference a child's first name. Online filenames must not identify children. Where possible group photographs are preferable to those of individual children.

Images of children may only be uploaded online by staff if parents/carers have given their permission for this.

Images/video of children can only be taken on Academy devices and then must be stored securely on the school network, never on personal devices such as mobile phones.

A pupil's personal space within any network/online environment should not host any inappropriate images. It is highly recommended that parental/carer approval is required re. any home uploading.

Images used to identify children in any external online community should be representative of the child (e.g. an avatar or symbol) rather than photographic.

8.1 Photographs and video – Parents/Carers
Parents/carers are welcome to take photographs at school performances and events under the following terms and conditions:
- Photographs should primarily be of the parent/carer's own child/children
- The photographs taken should be for family/close friends sharing
- Excepting 'prints' the photographs should not be published in any manner
  This includes any website or public social networking site publication

The videoing of parent/carer's children may take place unless an issue such as performance copyright exists. Staff will inform parents/carers prior to an event and at the start of each event if videoing is allowed. If videoing is permitted the conditions are as above for photography.

Outside of performances and events parents/carers are requested to ask a member of staff's permission before taking any photographs or videos at the Academy (conditions as above).

9. Filtering and safeguarding measures
Our Academies broadband connectivity has strict filtering systems to resist the delivery of inappropriate content (including extremist and terrorist materials). Anti-virus and spyware software is on our networks and updated on a regular basis. A firewall is used to protect our networks, including all information about children, from access by unauthorised users. Our wireless networks have encryption codes to resist hacking.

Our Academy websites host the CEOP 'Report Abuse' and Childline buttons. Children are taught the purpose of these and the 'report abuse' buttons in other online communities both to protect themselves and others.

10. Support
e-Safety teaching for pupils will take place at a classroom and key stage level on a termly basis and as required. Updates for parents/carers will be regularly shared via Seesaw, Academy's social media channels and websites.

Appendices

1. Digital Technologies - Acceptable and Expected Use Rules for Staff

To ensure that all adults within the Trust are aware of their responsibilities when using any digital/online technologies they are asked to sign their agreement to specific Acceptable Use Rules.
This is both to provide an example to children regarding safe and responsible use and as a safeguard from any potential allegations or inadvertent personal misuse.
These rules apply to all digital/online technology usage and to anything that may be downloaded or printed.

General:
- I have been given access to the Acceptable Use Policy to refer to for e-safety procedures I should follow.
- I will only use Trust/Academy equipment in an appropriate manner and for professional uses.
- I will adhere to copyright and intellectual property rights.
- I know that I should not be using Academy systems for personal use unless agreed by a Senior Manager.
- I will take measures or seek advice to prevent the potential introduction of viruses to the network.
- I will exercise caution when following links/opening attachments within emails, alert to signs of cyber-attack
- I will ensure that I keep all passwords secure and try not to leave any machine 'logged in'.
- I will report any accidental misuse and report any incidents of concern to a Senior Manager.

Photographs, Video & Mobile file storage:
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet and will need to approve content uploaded by pupils to Seesaw.
- I know that all Academy images should appropriate and beyond first names not reveal any personal information about children if uploaded to the internet.
- I must only use equipment provided by the Academy. Media taken on Trust/Academy devices should be transferred to the school network or Seesaw as soon as is possible. Any use of personal equipment, including mobile phones, for taking photographs/video is strictly prohibited.
- I must only use Academy provided USB memory sticks and follow agreed encryption procedures. I will not download, copy or store any school personal data (including pupil photographs) to a personal device.

Communication & Social Networking:
- I will only use my Academy email address for work-related communications.
- I will ensure all messages are written carefully and politely (emails can be forwarded to unintended readers) and will secure any emails or password protect any email attachments which contain personal information.
- I will never use a personal phone to contact pupils and only if directed to/with my number blocked, to contact parents. I will not communicate with parents directly via my school email address – all such communication must be through the official Academy contact email address.
- I realise that I am putting myself at risk of misinterpretation and allegation should I contact children via any systems other than Academy provided ones. I will not use any non-Academy online technologies to communicate with pupils. Specifically, I will not accept or request the 'friendship' of pupils.
- I understand the value of setting my 'Privacy' settings appropriately on any social networking site and not stating my place of work – this will help to prevent unacceptable 'friendship' requests.
- I will not risk bringing the Trust/my Academy into disrepute by 'discussing any aspect of my work or by making any Trust/Academy related comments or references' online (or by any means to non-Academy personnel, to ensure others do not do the same) other than (as delegated) via official Trust/Academy web presence agreed protocols.

- I have read, understood and will follow the Trust's 'Acceptable and Expected Use of Digital Technologies Policy' and the rules specified above.
- I understand my responsibilities regarding safeguarding children when digital/online technologies are used.

Signed: _____   Date: _____

Name (printed): _____

2. <u>Procedures Following Staff Misuse or Incident</u>

Principals/Senior Trust Managers will ensure these procedures are followed, in the event of misuse or incident:

A.   **An inappropriate website is accessed accidentally:**
     Report incident /website to the e-Safety Leader.
     e-Safety Leader to log and update filtering service.

B.   **An inappropriate website is accessed deliberately:**
     Ensure that no one else can access the material by switching off display.
     If possible, preserve any evidence.
     Report to the e-Safety Leader and Principal immediately.
     Contact Police or other agencies
           (including the Channel Scheme re. radicalisation) as necessary.
     Decide on appropriate disciplinary response.
     e-Safety Leader to log and update filtering services.

C.   **A staff member receives inappropriate material:**
     Do not forward this material to anyone else – doing so could be an illegal activity.
     Alert the e-Safety Leader and Principal immediately.
     e-Safety Leader to preserve any evidence and log the nature of the material.
     Contact Police or other agencies, as for B.

D.   **A staff member has used ICT equipment inappropriately:**
     Ensure that no one else can be affected by the activity.
     If possible, preserve any evidence.
     Report to the e-Safety Leader and Principal immediately.
           If involving children report to Designated Person for Child Protection
           follow Child Protection Policy and inform parents/carers.
     Contact Police or other agencies, as for B.
     Decide on appropriate disciplinary response.

E.   **A staff member has communicated with a child inappropriately:**
     Ensure the child is reassured and remove them from the situation immediately.
     Report to the Principal, Designated Person for Child Protection and e-Safety Leader.
     Preserve the information received by the child if possible.
     Principal to follow the Allegation Procedure and/or Child Protection Policy.
     Notify parents/carers.
     Contact CEOP / Police or other agencies, as for B.
     Decide on appropriate disciplinary response.

F.   **Inappropriate, damaging, malicious or threatening comments/files are posted online:**
     Preserve any evidence. Support any individuals affected.
     Inform the e-Safety Leader and Principal immediately.
     Investigate. Decide on appropriate remedial actions.
     Contact Police or other agencies as for B.
     If posted by staff member decide on appropriate disciplinary response.

G.   **Any misuse or breach of the acceptable use policy which may risk the security of any personal data should be reported to the Data Protection Officer, Debbie Pettiford.**

3. <u>Procedures Following Pupil Misuse or Incident</u>

Principals will ensure these procedures are followed, in the event of misuse or incident:

A.   **An inappropriate website is accessed accidentally:**
Reassure the child that they are not to blame and praise them (or 'informant' peer)
for being safe and responsible by telling an adult.
Report incident /website to the e-Safety Leader.
Decide if parents/carers need to be notified.
e-Safety Leader to log and update filtering service.

B.   **An inappropriate website is accessed deliberately:**
Refer the child to the Internet Usage Agreement.
Report incident /website to the e-Safety Leader.
Decide on appropriate sanction.
e-Safety Leader to log and update filtering service.
Notify parents/carers plus Principal, Designated Person for Child Protection,
external agencies (including the Channel Scheme re. radicalisation) as necessary.

C.   **A child has received an inappropriate communication:**
Ensure the child is reassured and remove them from the situation immediately.
Preserve the communication/all related evidence as received by the child.
Report to the Principal, Designated Person for Child Protection
and e-Safety Leader.
Follow the Child Protection Policy.
Notify parents/carers plus contact CEOP / Police and other agencies, as for B.

D.   **Inappropriate, upsetting, malicious or threatening comments/files are posted online:**
Preserve all related evidence. Support any individuals affected.
Report to the Principal, Designated Person for Child Protection
and e-Safety Leader.
Decide on appropriate remedial actions.
If posted by a child decide on appropriate sanctions.
Notify parents/carers and other agencies, as for B.

E.   **Any misuse or breach of the acceptable use policy which may risk the security of any personal data should be reported to the Data Protection Officer, Debbie Pettiford.**

N.B. There are three events which must be reported directly to the police:
- Indecent images of children found.
- The sending of obscene materials to a child.
- Suspicion of 'grooming' behaviour.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if such an event occurs. If in doubt, do not power down the machine.

It is important to remember that any offensive images that may be encountered should never be forwarded to anyone else - even if it is to report them as illegal, as the forwarding itself may constitute illegal activity and could bring liability to prosecution and investigation by the police.

4. Digital Technologies - Acceptable and Expected Use Rules for Staff
Abridged - for short-term staff / volunteers / work experience students

To ensure that all adults within the Trust are aware of their responsibilities when using any digital/online technologies they are asked to sign their agreement to specific Acceptable Use Rules.
This is both to provide an example to children regarding safe and responsible use and as a safeguard from any potential allegations or inadvertent personal misuse.
These rules apply to all digital/online technology usage and to anything that may be downloaded or printed.

General:
- I will only use Trust/Academy equipment in an appropriate manner and for professional uses.
- I will adhere to copyright and intellectual property rights.
- I know that I should not be using Academy systems for personal use unless agreed by a Senior Manager.
- I will take measures or seek advice to prevent the potential introduction of viruses to the network.
- I will ensure that I keep all passwords secure and try not to leave any machine 'logged in'.
- I will report any accidental misuse.
- I will report any incidents of concern to a Senior Manager.

Photographs & Video:
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet and will need to approve content uploaded by pupils to Seesaw.
- I know that all Academy images should appropriate and beyond first names not reveal any personal information about children if uploaded to the internet.
- I will not take images on any personal devices at the Academy.
- I will not download, copy or store any school personal data (including pupil photographs) to a personal device.

Communication & Social Networking:
- I realise that I am putting myself at risk of misinterpretation and allegation should I contact children via any systems other than Academy provided ones. I will not use any non-Academy online technologies to communicate with pupils. Specifically, I will not accept or request the 'friendship' of pupils.
- I understand the value of setting my 'Privacy' settings appropriately on any social networking site and not stating my place of work – this will help to prevent unacceptable 'friendship' requests.
- I will not risk bringing the Academy into disrepute by 'discussing any aspect of my work or by making any Academy related comments or references' online (or by any means to non-Academy personnel, to ensure others do not do the same).

- I have read, understood and agree to follow the Trust's rules as specified above.

- I understand my responsibilities regarding safeguarding children
  when digital/online technologies are used.

Signed: _____   Date: _____

Name (printed): _____