


The Harmony Project Online Safety Policy

Lead	The Harmony Project Leadership Team
Policy prepared by	Clare Long
Policy approved by Director	Richard Dunne
Signed by Director	
Operational from	1 st June 2025
Due for review	April 2026
Reviewed by and on	Julia Jones, June 2025

Statement of Intent: The Harmony Project understands that using online services is an important aspect of raising educational standards, enhancing teaching and learning within a school and running smooth operations as a charity. The use of online services is embedded throughout the schools we work with and how we operate as a charity, therefore there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, cyberbullying and bringing The Harmony Project's reputation into disrepute.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect staff and the communities that we interact with, through our work, revolve around these areas of risk. Our charity has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all.

Contents:

1. Legal Framework
2. Roles and responsibilities
3. Managing online safety
4. Cyberbullying
5. Grooming and exploitation
6. Mental health
7. Online safety training for staff
8. Online safety and the curriculum
9. Use of technology in the classroom
10. Internet access
11. Filtering and monitoring online activity
12. Network security
13. Emails
14. Generative artificial intelligence (AI)
15. Social networking
16. The Harmony Project website
17. Use of devices
18. Monitoring and review

Appendix

- 1 Acceptable Use Agreement

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 • DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes' • DfE (2024) 'Keeping children safe in education 2024'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following policies:

- The Harmony Project [Social Media Policy](#)
- The Harmony Project [Safeguarding and Child Protection Policy](#)
- The Harmony Project [Staff Code of Conduct](#)

2. Roles and responsibilities

The Board of Trustees and Chair are responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.

- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that appropriate levels of security are in place.
- Ensuring that the security measures are reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the Leadership Team and other relevant staff have an awareness and understanding of the security measures, manage them effectively and know how to escalate concerns when identified.

The DSL is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout The Harmony Project's policies and procedures, including in those related to safeguarding.
- Allocating enough time, support and resources to carry out DSL responsibilities in relation to online safety.
- Ensuring staff receive regular up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are maintained.
- Supporting staff to ensure that an awareness of online safety is embedded within the Harmony curriculum and linked resources.
- Taking the lead responsibility for online safety in the charity and ensuring that all staff are aware of their responsibilities when in schools and other educational settings.
- Undertaking training so the risks associated with online safety, and additional risks that pupils with SEND face online, are understood and recognised.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO at a school and ICT technicians.
- Ensuring online safety is recognised as part of the charity's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the charity's approach to remote learning.
- Understanding the security measures in place at The Harmony Project.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation the online security measures at the charity.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.

- Understanding the purpose of record keeping.
- Monitoring online safety incidents to identify trends and any gaps in the charity's provision, and using this data to update the charity's procedures.
- Reporting to the Board of Trustees about online safety on a termly basis as part of the Safeguarding update.
- Working with the Board of Trustees to update this policy on an annual basis.

Our ICT contractor, Implicit Limited is tasked by the DSL to:

- Provide general technical support in connection with the development and implementation of the charity's online safety policies and procedures.
- Implement appropriate security measures as instructed by the DSL.
- Ensure that the charity's security measures are updated as appropriate as instructed by the DSL.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the charity and individual school's reporting procedure.

This statement is applicable to all references made to Implicit throughout this document: Implicit Limited are not responsible or accountable for your security. The responsibility lies with The Harmony Project who can instruct Implicit Ltd to take action.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the charity's approach to online safety, with support from the DDSL and Head of Business Development & Operations where appropriate, and will ensure that there are strong processes in place to handle any concerns about safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all operations in the following ways:

- Staff receive regular training
- Staff receive email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is addressed, where appropriate, within the design of our curriculum

Handling online safety concerns

Any disclosures made about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another, will be handled in line with [The Harmony Project Safeguarding & Child Protection Policy](#).

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that persons displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

Concerns regarding a staff member's online behaviour are reported to the DSL, who decides on the best course of action in line with the relevant policies, e.g. [The Harmony Project Staff Code of Conduct](#). If the concern is about the Director, it is reported to the Chair of Trustees.

Concerns regarding a pupil's online behaviour are reported to the DSL within the child's school.

All online safety incidents and the school's/charity's response are recorded by the DSL in [The Harmony Project Safeguarding Incident Record](#) found within [The Harmony Project Safeguarding and Child Protection Policy](#).

4. Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The Harmony Project will be aware that certain staff and pupils within a school context can be more at risk of abuse and/or bullying online, such as LGBTQ+ and those with SEND.

Cyberbullying against staff, or pupils within a school context, is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur, in line with [The Harmony Project Staff Code of Conduct](#) and [Safeguarding and Child Protection Policy](#).

5. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils/staff who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil/member of staff may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are

Where charity staff have any concerns about staff within the organisation with relation to grooming, they will bring these concerns to the DSL without delay. The DSL will manage the situation in line with [The Harmony Project Safeguarding and Child Protection Policy](#).

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation. Where staff have a concern about a pupil relating to radicalisation, they will report this to the school's DSL without delay, who will handle the situation in line with the school's Prevent Risk Assessment.

6. Mental health

Staff will be aware that online activity both in and outside of work/school can have a substantial impact on a person's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a staff member is suffering from challenges in their mental health. Concerns about the mental health of a staff member will be addressed by the Head of Business Development & Operations. Concerns about the mental health of a pupil within a school will be addressed by the school's pastoral support team.

7. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to the security measures in place. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

8. Online safety and the curriculum

An awareness of online safety is embedded throughout the Harmony curriculum; however, it is particularly addressed in the following subjects/ areas:

- PSHE (including RSE and Health education)
- Citizenship – through assemblies

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy.

The online risks pupils may face online are always considered when developing the curriculum. Staff review external resources prior to using them, to ensure they are appropriate for the cohort of pupils for which the curriculum materials have been designed.

9. Use of technology in the classroom

A wide range of technology may be used during lessons/ sessions/ workshops/ assemblies/ training with the Harmony Project, including the following:

- Laptops
- Tablets (iPads)
- Local network
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom/learning environment, or recommending that staff or pupils use these tools or platforms at home, the Harmony Project member of staff will always review and evaluate the resource. Harmony Project staff ensure that any internet-derived materials are used in line with copyright law. The Harmony Project Team will advise that pupils should be supervised when using online materials during lesson/activity time – this supervision should be suitable to their age and ability and individual school policies.

10. Internet access

When visiting a school or other educational establishment, Harmony Project staff are expected to read and sign the [local Acceptable Use Agreement](#) to be granted access to the establishment's internet network. It is good practice and we encourage Harmony staff to use the school's internet network, instead of mobile networks, as the school's network will have appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

11. Filtering and monitoring online activity

The Board of Trustees ensure the charity's ICT network has appropriate security measures in place. The Board of Trustees ensure 'over blocking' does not lead to unreasonable restrictions.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage the charity's security systems and to ensure they meet the charity's safeguarding needs.

The Head of Business Development & Operations and ICT support undertake a risk assessment to determine what security systems are required. ICT support will undertake regular checks on the security systems to ensure they are effective and appropriate.

Requests regarding making changes to the security systems are directed to the DSL. Prior to making any changes to the security systems, ICT support and the DSL conduct a risk assessment. Any changes made to the system are recorded by ICT support. Reports of inappropriate websites or materials are made to the DSL immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the security systems will be reported to the DSL, who will escalate the matter appropriately. If a member of staff has deliberately breached the security systems, it will be dealt with in line with [The Harmony Project Staff Code of Conduct](#).

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The charity's network and charity-owned devices will be subject to ad hoc checks. All users of the network and charity-owned devices will be informed about how and why they are checked. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with [The Harmony Project Safeguarding and Child Protection Policy](#).

12. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the ICT support consultancy (Implicit). Software firewalls are switched on at all times. ICT technicians will review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

The Harmony Project maintains and renews the government-backed cyber security certification known as 'Cyber Essentials' on an annual basis (as displayed by the badge on The Harmony Project website).

Staff are instructed to be vigilant when working with email and web browsers. In particular, they are instructed to be suspicious of unfamiliar email senders, especially when presented with email attachments and/or links. Staff are expected to immediately report any suspicious content or if there is any reason to believe that their computer or email account may have been compromised to the Head of Business Development & Operations who will instruct Implicit Limited to take the appropriate action.

The Harmony Project has a procedure in place in the event of a suspected email account being compromised – this procedure involves immediate actions/notifications, internal and external handlings.

In the event of a notifiable security breach, the Head of Business Development & Operations has a duty of care to inform the Information Commissioner's Office within 72 hours.

In the event of a phishing incident, Implicit Limited are to report the phishing attempt to the National Cyber Security Centre (NCSC). Staff are encouraged to do the same.

All members of staff have their own unique usernames and passwords to access the systems of the charity. Staff members are responsible for keeping their passwords private. There is a compulsory format and policy for all passwords: each password is unique and recycling of passwords is not permitted, use of a pass-phrase using 3 words that are random and not related to the person or the account in any way, all passwords must be a minimum of 12 characters with no maximum set, all passwords must have a minimum of 1 of the following: upper case, lower case, number, special character. The Harmony Project recommends all staff use the passphrase generator tool (found on the Implicit website) to support with the creation of new passwords to ensure they are as secure as possible.

Users inform ICT support if they forget their login details, who will arrange for the user to access the systems under different login details.

Staff users are required to lock access to devices and systems when they are not in use.

Staff are required to save all Harmony Project related work to THP Share Point for security purposes and for use as a collective resource.

Daylite user staff members are expected to record and maintain all client contact details and communication by using The Harmony Project's Daylite CRM system. This includes:

- Contact information including phone, email and address
- Email communication using the Daylite Mail Assistant
- Tasks
- Shared Daylite Calendar
- Daylite Notes for updating details about communication and updates with contacts during the course of working with The Harmony Project.

Staff should not use separate spreadsheets or other notes or tasks systems for managing lists of clients/contacts etc.

13. Emails

Staff members are required to block spam and junk mail, and report anything suspicious to ICT support. If staff receive suspicious links, malware and profanity within emails they are required to report the matter to the Head of Business Development & Operations who will instruct Implicit Limited to take the appropriate action for ICT support. Spam and all other emails from unknown sources should be deleted without clicking on links contained within.

The Head of Business Development & Operations will update staff where they explain what a phishing email and other malicious emails might look like – this could include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking “does the email urge you to act immediately?”
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails or any other means will be managed and coordinated by the Head of Business Development & Operations who will instruct Implicit Limited to take the appropriate action.

As detailed in section 12. Network Security, In the event of a notifiable security breach, the Head of Business Development & Operations has a duty of care to inform the Information Commissioner's Office within 72 hours. In the event of a phishing incident, Implicit Limited are to file a report with the National Cyber Security Centre. Staff are encouraged to do the same.

14. Generative artificial intelligence (AI)

The Harmony Project will take steps to prepare staff for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to the nature of our work. The charity will ensure its IT system includes appropriate security measures to limit the ability to access or create harmful or inappropriate content through generative AI. Through the ad hoc monitoring checks the charity will ensure that staff are not accessing or creating harmful or inappropriate content, including through generative AI. The charity will take steps to ensure that personal and sensitive data is not entered into generative AI tools. The Harmony Project will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

15. Social networking

The use of social media by staff and pupils will be managed in line with [The Harmony Project Social Media Policy](#).

16. The Harmony Project website

The Head of Business Development & Operations is responsible for the compliance of the overall content of the charity website and ensuring that it meets government requirements. The Head of Content Development will ensure the content is appropriate, accurate and up to date. The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff or schools is not published on the website. Images and videos are only posted on the website if

permission has been given from the school and parent as part of the [Image Consent Form](#) within [The Harmony Project Social Media Policy](#).

17. Use of devices

Charity-owned devices

Salaried staff members may be issued with a laptop to assist with their work, on a case-by-case basis.

Charity-owned devices are used in accordance with the [Acceptable Use Agreement](#) and are configured in line with the Cyber Essentials framework.

ICT support periodically review charity-owned devices to ensure there is no inappropriate material or malware on the devices.

Cases of staff members found to be misusing charity-owned devices will be managed in line with the [Acceptable Use Policy](#) and [The Harmony Project Staff Code of Conduct](#).

Personal devices

Any personal electronic device is the responsibility of the user. Personal devices will be required to be configured in line with the Cyber Essentials framework; staff will be made aware of this as part of their induction to the organisation.

When in school establishments, Harmony Project staff's personal electronic devices should only be used in the staff room, a meeting room or office and must not be used when they are with pupils, except in an emergency.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils. Harmony Project cameras or photographers can be used to record images following agreement from the school and adherence to [image and social media policies](#).

Staff members should report concerns about their colleagues' use of personal devices on any school/educational setting in line with [The Harmony Project Whistleblowing Policy](#). If a member of

staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the DSL will inform the police and action will be taken in line with [The Harmony Project Whistleblowing Policy](#).

18. Monitoring and review

The charity recognises that the online world is constantly changing; therefore, the DSL, Board of Trustees and ICT support will review this policy in full on an annual basis and following any online safety incidents. Any changes made to this policy are to be communicated to all members of staff.

Appendix 1. Acceptable Use Agreement

This Acceptable Use Agreement is quoted in [The Harmony Project Code of Conduct](#) and must therefore be adhered to at all times. The agreement is intended to ensure that:

- All staff, Trustees and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.
- The charity ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff, Trustees and volunteers are protected from potential risk in their use of ICT in their everyday work.

Acceptable Use Agreement

- I understand that I must use the charity's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing the work of the charity and learning in education. I will, where possible, embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the charity will monitor the use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of charity's ICT hardware and systems (e.g. laptops, email etc) out of working hours.
- I understand that the charity's ICT hardware and systems are primarily intended for the charity's day-to-day operational use.
- I am responsible for keeping my username and passwords private.
- I understand that there is a compulsory format and policy for all passwords: each password is unique and recycling of passwords is not permitted, use of a pass-phrase using 3 words that are random and not related to the person or the account in any way, all passwords must be a minimum of 12 characters with no maximum set, all passwords must have a minimum of 1 of the following: upper case, lower case, number, special character. I will use the passphrase generator tool (found on the Implicit website) to support with the creation of new passwords to ensure they are as secure as possible.

- I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the DSL or Head of Business Development & Operations.

I will be professional in my communications and actions when using the charity's ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will not delete any resources produced for charity use unless they have been updated.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the [Image Consent Forms](#) and the charity's policy on the use of digital/video images (detailed in [The Harmony Project Social Media Policy](#)). I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the charity's website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use social networking sites when in a school environment.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner. I will not give students my personal email address.
- I will not contact any students via a social networking site and will ensure that there is nothing inappropriate on the public profile of my social networking site.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

When in a school/educational environment, the establishment has the responsibility to provide safe and secure access to technologies and ensure their smooth running:

- When I use my personal handheld/external devices (tablets/laptops/mobile phones/USB devices etc.) in a school, I will follow the rules set out in this agreement.
- I will be vigilant and not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up by accepting all software updates.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.

- I will not try to use any programs or software that might allow me to bypass the security systems in place to prevent access to such materials.
- I will not disable or cause any damage to charity equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not store any personal data which includes details of students on any personal devices.

When using the internet in my professional capacity:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of my working environment:

- I understand that this Acceptable Use Policy applies not only to my work and use of ICT equipment in schools and other educational establishments, but also applies to my use of the charity ICT systems and equipment out of work hours and my use of personal equipment in school or in situations related to my employment.
- I understand that if I fail to comply with this Acceptable Use Policy there will be, referral to Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

Declaration of receipt

I confirm that I have read **The Harmony Project Online Safety Policy, The Harmony Project Staff Code of Conduct and Acceptable Use Policy and Guidance for Safer Working Practice for those working with children and young people in education settings, February 2022** and understand that any unlawful or unsafe behaviour could lead to appropriate legal or disciplinary action being taken.

Name: (please print):

Signature: Date:

Please return this slip to the Head of Business Development & Operations as soon as possible.

USEFUL CONTACTS

Richard Dunne 07872 959 334 (24 hours)	Director of Education and DSL richard@theharmonyproject.org.uk
Catherine Smith 07920 460 056	Head of Schools & Outreach & Deputy DSL catherine@theharmonyproject.org.uk
Julia Jones 07710 197 187	Head of Business Development & Operations julia@theharmonyproject.org.uk
Clare Long 07976 371 489	Events & Project Coordinator clare@theharmonyproject.org.uk