Online Safety & Safeguarding

Reviewed: Nov 2022

Reviewed:	21/11/2022
Expiry Date:	21/11/2023
Next Review:	May 2023
Annual Appraisal:	August 2023

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

Online Safety & Safeguarding

TABLE OF CONTENTS

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

1.0 Introduction

There is a duty of care required for the By Design Group Ltd and associated companies (BDG for future reference in this document) to create an online atmosphere where all children, young people and vulnerable adults are provided with a safe place where they all feel valued and welfare is promoted.

BDG are committed to safeguarding and promoting the welfare of young people and adults at risk. We require that all staff, volunteers, participants, any partner agencies, or any commissioned service providers who have access to and are users of BDG digital technology systems, share this commitment.

This commitment extends to all BDG and covers all Learn and NCS online activities including and not limited to its holistic education activities.

This policy should be read alongside BDG policies and procedures on safeguarding:

- DBS Disclosures Security Policy - LBD14A
- Safeguarding Policy - LBD44A
- Social Media Policy - LBD45A
- Involving Volunteers and Student Helpers - LBD49A
- Vulnerable Adults - LBD50A
- Safer Recruitment Policy - LBD61A

Code of Conducts linked to the policy:

- Safeguarding and Child Protection Code of Conduct – LBD78P
- Social Medi Code of Conduct - LBD79P
- Online Safety Code of Conduct – LBD80P
- Webinars Safety Code of Conduct - LBD81P

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

2.0 Policy Context

The By Design Group Ltd and associated companies (BDG for future reference in this document) adopt and adhere to the following policy.

This Online Safety & Safeguarding policy refers to all BDG online education activities.

The BDG will review its Online Safety & Safeguarding policy on an annual basis and check that it and its staff and associates, where appropriate, are adhering to the policy and will undertake to act wherever possible to meet best Safeguarding practices.

The purpose of this policy statement is to:

- Ensure that the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media, or mobile devices.
- Provide staff and volunteers with the overarching principles that guide our approach to online safety.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

2.1 Legal Framework

- This policy has been drawn up based on legislation, policy and guidance that seeks to protect children in England, Northern Ireland, Scotland, and Wales.
- Summaries of the key legislation and guidance are available on:
    - online abuse, https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
    - bullying, https://learning.nspcc.org.uk/child-abuse-and-neglect/bullying
    - child protection, https://learning.nspcc.org.uk/child-protection-system

2.2 BDG Believe That:

- Children and young people should never experience abuse of any kind.
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are always kept safe.

2.3 BDG Recognise That:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges.
- BDG have a duty to ensure that all children, young people, and adults involved in our organisation are protected from potential harm online.
- BDG have a responsibility to help keep children and young people safe online, whether or not they are using BDG network and devices.
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation, have the right to equal protection from all types of harm or abuse.

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

- Working in partnership with children, young people, their parents, carers, and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

3.0 Roles and Responsibilities

3.1 Program Managers / Leaders

- The Program Manager / Leader has a duty of care for ensuring the safety (including online safety) of learners and service users, though the day to day responsibility for online safety will be delegated to the Designated Person.
- The Program Managers / Leaders and Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against the BDG and / or a member of staff.
- The Senior Management Team are responsible for ensuring that the Program Managers / Leaders and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other members of BDG staff, as relevant.
- The Program Managers / Leaders and Senior Management Team will ensure that there is a system in place to allow for monitoring and support of those in the BDG who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those BDG staff members who take on important monitoring roles.

3.2 BDG Online Content Providers

- BDG Online Content Providers take the day-to-day responsibility for online safety issues and have a leading role in establishing and reviewing the BDG online safety policies / documents.
- BDG Online Content Providers ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- BDG Online Content Providers will provide training and advice for staff.
- BDG Online Content Providers will liaise with KIXO (ICT service provider) technical staff.

3.3 Network Manager / Technical Staff

BDG has the responsibility to ensure that KIXO (ICT service provider), carries out all the online safety measures that would otherwise be the responsibility of the BDG technical staff.

Those with technical responsibilities are responsible for ensuring:

- That the BDG technical infrastructure is secure and is not open to misuse or malicious attack.
- That the BDG meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply.
- That BDG system users may only access the networks and devices through properly enforced password protection.

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the networks / internet / digital technologies is regularly monitored in order that any misuse / attempted misuse can be reported to the Senior Management Team; Program Managers / Leaders for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed with the BDG.

3.4 BDG Staff

BDG staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current BDG online safety policy and practices.
- They have read, understood BDG policies.
- They report any suspected misuse or problem to the Program Managers / Leaders for investigation / action / sanction.
- All digital communications with learners / service users / parents / carers should be on a professional level and only carried out using official BDG systems.
- Online safety issues are embedded in all aspects of the BDG activities.
- They monitor the use of digital technologies, mobile devices, cameras, etc. in education and other BDG activities (where allowed).
- In BDG pre-planned online activities learners / service users should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found on the internet.

3.5 Parents / Carers

- Parents / carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The BDG will take every opportunity to help parents understand these issues through website and social media information.
- Parents and carers will be encouraged to support the BDG online activities in promoting good online safety practice and to follow guidelines on the appropriate use of:
    - Digital and video images taken at BDG events.
    - Their children's personal devices (where this is allowed).

3.6 Community Users

Community Users who access BDG systems or programmes as part of the wider BDG provision will be expected to follow BDG online system directions.

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

4.0 Designated Person

The Designated Person is the member of the Learn by Design management team who has specific responsibilities for ensuring effective safeguarding and protection procedures. **Please contact the Executive Chairman, Geoff Parsons, for all initial enquiries with regard to designated person.**

The role of the Designated Person is to:

- Receive and record information from staff, volunteers, children, or parents / carers who have protection concerns.
- Assess the information properly and carefully, clarifying or obtaining more information about the matter as appropriate and consulting with senior colleagues if necessary.
- Consult initially (or via a delegated project manager or member of staff) with the statutory child protection agency without delay.

5.0 Key Contact Details

Please contact the Executive Chairman, Geoff Parsons, for all initial enquiries with regard to designated person.

Geoff Parsons – By Design Group Chairman

Office: 01827 316297

Mobile: 07770 452161

Email: geoffparsons@bydesign-group.co.uk

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

Staffordshire - Local Authority Designated Officer (LADO) for Safeguarding:

Telephone: 01785 278958 or 01785 278997

Staffordshire County Council's First Response Service:
Telephone: 0800 1313 126

Open: Monday - Thursday 8:30am - 5:00pm
Friday 8:30am - 4:30pm
E-mail: firstr@staffordshire.gov.uk

Emergency Duty Service:
(Out of Hours Service)
Telephone: 0345 6042886

Local Children's Social Care

Tamworth Area Office

Marmion House
Lichfield Street
Tamworth, B79 7BZ

Tel:	0300 111 8010
Fax:	01827 475515
Sensory Phone (Hearing Impairments):	07976 191448
Minicom:	01827 475510
E-mail:	tamworth.socialservices@staffordshire.gov.uk

Opening Hours

Monday: 8.30am - 5.00pm
Tuesday: 8.30am - 5.00pm
Wednesday: 8.30am - 5.00pm
Thursday: 8.30am - 5.00pm
Friday: 8.30am - 4.30pm
Saturday: Closed
Sunday: Closed

Out of Hours contact: Emergency Duty Service 07815 492613

Alternatively, in an emergency you can contact Staffordshire Police Central Referral Unit on 101 or dial 999

Please note that similar details and numbers are available for all areas of the country that we work in via the Internet. If in doubt, please contact your line manager or designated safeguarding officer.

6.0 Policy Statements

6.1 Technical – Infrastructure / Equipment, Filtering and Monitoring

BDG has the responsibility to ensure that KIXO (ICT service provider) carries out all the online safety measures that would otherwise be the responsibility of the BDG.

The BDG will be responsible for ensuring that the BDG infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- BDG technical systems will be managed in ways that ensure that the BDG meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of BDG technical systems.
- Servers, wireless systems, and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to BDG technical systems and devices.
- All users will be provided with a username and secure password by KIXO who will keep an up-to-date record of users and their usernames.
- Users are responsible for the security of their username and password.
- KIXO is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

6.1.1 Internet Access (is filtered for all users)

- Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.
- There is a process in place to deal with requests for filtering changes.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the BDG systems and data.
- The BDG infrastructure and individual devices are protected by up to date virus software.
- An agreed provision of temporary access of "guests" (e.g., trainers, visitors) onto the BDG.

6.2 Mobile Technologies

Mobile technology devices may be BDG owned / provided or personally owned and might include smartphone, tablet, notebook / laptop, or other technology that usually has the capability of utilising the BDG wireless network. The device then has access to the wider internet which may include the BDG learning platform and other services such as email and data storage.

All users should understand that the primary purpose of the use of mobile / personal devices in a BDG context is work / educational.

6.3 Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to BDG learning activities, allowing BDG staff and learners / service users instant use of images that they have recorded themselves or downloaded from the internet. However, BDG staff, parents / carers and learners / service users need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the shorter or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The BDG will inform and educate users about these risks and will endeavour to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate learners / service users about the risks associated with the taking, using, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of learners / service users are published on the BDG website / social media / local press.
- BDG staff and volunteers are allowed to take digital / video images to support BDG aims, but must follow BDG policies concerning the sharing, distribution, and publication of those images. Those images should only be taken on BDG approved equipment.
- Care should be taken when taking digital / video images that learners / service users are appropriately dressed and are not participating in activities that might bring the individuals or the BDG into disrepute.
- Learners / service users must not take, use, share, publish or distribute images of others without their permission.

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

- Photographs published on the website, or elsewhere that include learners / service users will be selected carefully and will comply with good practice guidance on the use of such images.
- Learners / service users' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Learners / service users work can only be published with the permission of the learners / service users and parents or carers.

7.0 Data Protection

By Design Group and associated companies are fully committed to compliance with the General Data Protection Regulation which came into force on the 25th of May 2018 which has direct effect across EU member states, starting from 25th May 2018. However, each country has the opportunity to make their own provisions for how it applies in their nation, hence the UK Data Protection Bill was created and came into force 23rd May 2018. We will therefore follow procedures that aim to ensure that all employees, volunteers, and other partners who have access to any personal data held by or on behalf of the company will follow:

- BDG Data Protection Policy & Procedures, LBD13A

8.0 Social Media - Protecting Professional Identity

The BDG provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners / service users, staff, and the BDG through:

- Ensuring that personal information is not published.
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.

8.1 BDG Staff Should Ensure That:

- No reference should be made in social media to learners / service users, parents / carers or BDG staff by name or any method of identification without prior approval.
- They do not engage in online discussion on personal matters relating to members of the BDG community.
- Personal opinions should not be attributed to the BDG.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

8.2 When Official BDG Social Media Accounts Are Established There Should Be:

- A process for approval by Program Managers / Leaders.
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff.
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under BDG disciplinary procedures.

8.3 Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the BDG or impacts on the BDG, it must be made clear that the member of staff is not communicating on behalf of the BDG with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the BDG are outside the scope of this policy.
- Where excessive personal use of social media in BDG is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The BDG permits reasonable and appropriate access to private social media sites.

8.4 Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the BDG.
- The BDG will effectively respond to social media comments made by others.

8.5 Dealing with Unsuitable / Inappropriate Activities:

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from BDG and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but would be inappropriate in a BDG context, either because of the age of the users or the nature of those activities.

The BDG believes that the activities referred to in the following section would be inappropriate in a BDG context and that users, as defined below, should not engage in these activities in/or outside the BDG when using BDG equipment or systems.

The BDG policy restricts usage as follows:

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

8.5.1 User Actions:

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals, or comments that contain or relate to:	Child sexual abuse images –The making, production, or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement, or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data, and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)						X
Using systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by the school/academy					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X		
Infringing copyright					X	
On-line gaming, shopping/commerce			X			
File sharing		X				
Use of social media			X			
Use of messaging apps		X				
Use of video broadcasting e.g. YouTube		X				

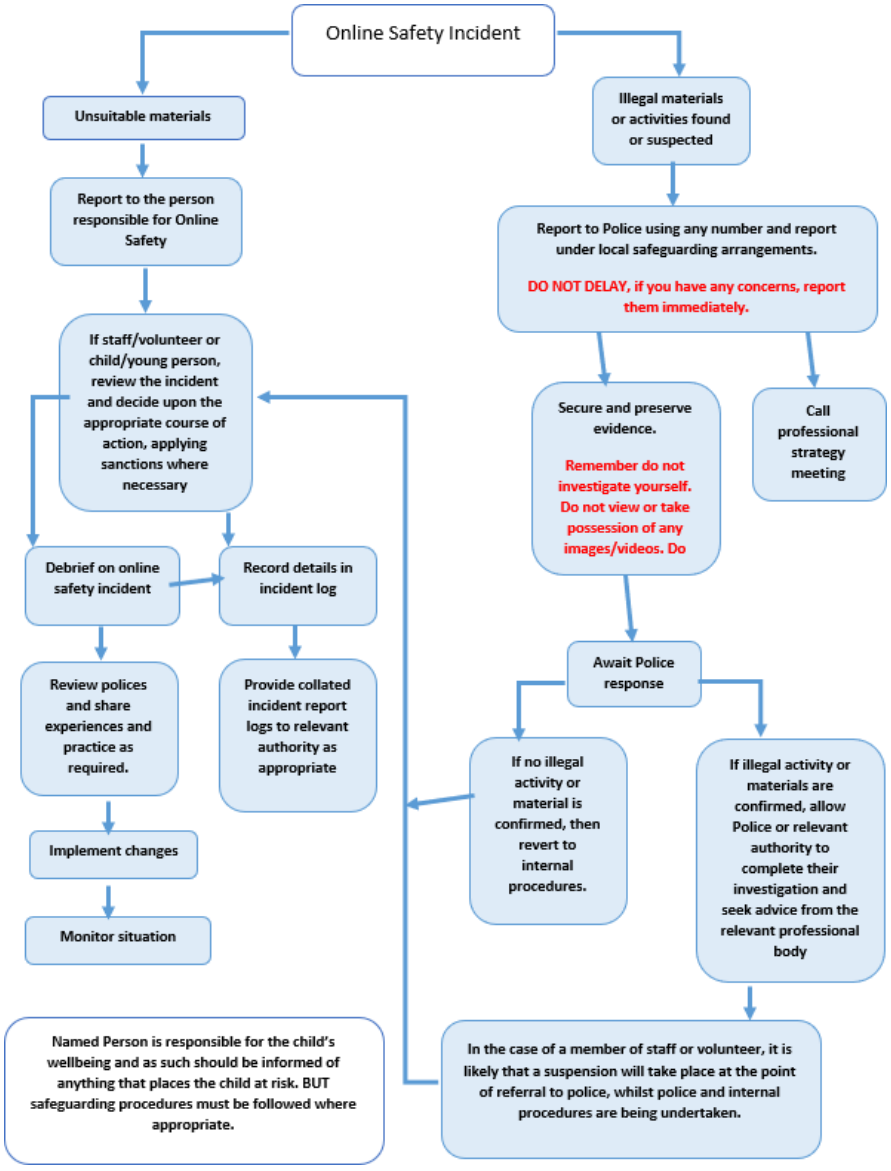
By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

9.0 Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

9.1 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

9.2 Other Incidents

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

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the BDG management team will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures.
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and / or action.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Promotion of terrorism or extremism.
- Offences under the Computer Misuse Act (see User Actions chart above).
- Other criminal conduct, activity, or materials.

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
It is important that all of the above steps are taken as they will provide an evidence trail for the BDG and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. Completed paperwork should be retained by the BDG management team for evidence and reference purposes.

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

9.3 BDG Staff & Learners / Service Users Actions & Sanctions

It is more likely that the BDG will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the BDG community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures:

9.3.1 Staff Incidents

	Refer to line manager	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff	Warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X	X			
Inappropriate personal use of the internet/social media/personal email					X	
Unauthorised downloading or uploading of files	X			X		
Allowing others to access BDG network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X			X		X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X			X		
Deliberate actions to breach data protection or network security rules	X			X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X		X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X				X	X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with learners/service users.	X	X	X		X	X
Actions which could compromise the staff member's professional standing	X				X	X
Actions which could bring the BDG into disrepute or breach the integrity of the ethos of the BDG	X				X	X
Using proxy sites or other means to subvert the BDG filtering system	X			X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X			X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X		X
Breaching copyright or licensing regulations	X				X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

Appendix

Managing Your Personal Use of Social Media:

- "Nothing" on social media is truly private.
- Social media can blur the lines between your professional and private life. Do not use the BDG logo and / or branding on personal accounts.
- Check your settings regularly and test your privacy.
- Keep an eye on your digital footprint.
- Keep your personal information private.
- Regularly review your connections – keep them to those you want to be connected to.
- When posting online consider: Scale, Audience and Permanency of what you post.
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

Managing BDG Social Media Accounts

The Do's

- Check with a line manager before publishing content that may have controversial implications for the BDG.
- Use a disclaimer when expressing personal views.
- Make it clear who is posting content.
- Use an appropriate and professional tone.
- Be respectful to all parties.
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author.
- Express opinions but do so in a balanced and measured manner.
- Think before responding to comments and, when in doubt, get a second opinion.
- Seek advice and report any mistakes.
- Consider turning off tagging people in images where possible.

The Don'ts

- Don't make comments, post content or link to materials that will bring the BDG into disrepute.
- Don't publish confidential or commercially sensitive material.
- Don't breach copyright, data protection or other relevant legislation.
- Consider the appropriateness of content for any audience of BDG accounts, and do not link to, embed, or add potentially inappropriate content.
- Don't post derogatory, defamatory, offensive, harassing, or discriminatory content.
- Don't use social media to air internal grievances.

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk