Bradford Learning Network

Code of Connection

CONTENTS

1 Introduction

The Bradford Learning Network (BLN) Code of Connection policy provides mandatory (**shall**) and best practise (**should**) protocols. This is for both legal and effective use of Information and Communication Technology (ICT) for accessing resources via the BLN.

The BLN encourages flexibility in how connected organisations approach teaching and learning through the use of ICT and aims to help its customers do this using the BLN services on offer.

All BLN customers **shall** meet the mandatory requirements and the customer **should** also ensure that relevant aspects of IT usage and legal obligations are covered under their Acceptable Use of ICT Policy (AUP). This is to provide a safe framework for using ICT, without exposing the BLN or its customers to the risks which can come with its use.

For the purpose of this Code of Connection, ***connected organisation*** refers to any type of site connected to the BLN who make use of its services, throughout this document the terms ***connected organisation*** and ***customer*** can be regarded as one and the same. A ***customer*** is likely but may not always be a school.

This Policy has been developed to:-

- ensure acceptable use of the internet by all users (as advised by the Internet Watch Foundation www.iwf.org.uk)
- establish the parameters of appropriate use and best practice
- protect the BLN, customer and users from potential legal liabilities
- explain the consequences of breaching acceptable use

This policy applies to all users of the BLN including, but not limited to:-

- full-time, part-time, term-time and any temporary staff
- pupils/students including full and part time
- third party organisations or contractors
- anyone appropriately authorised to access and use customer ICT facilities which subsequently connect to the BLN systems and services

The policy relates to the use of:-

- all devices including portable devices, all mobile communications devices such as Personal Digital Assistants (PDAs) and all Smartphones (regardless of ownership) when accessing the BLN
- ICT systems such as applications, e-mail and internet browsing where the BLN has a business interest or can be brought into disrepute through its misuse

This code of connection will be subject to amendment in response to changing circumstances and understanding. Should this occur, connected organisations will be advised accordingly.

2 Regulatory and Compliance Requirements

The customer **shall** be required to comply with all relevant legislation affecting ICT use, technology, security and standards. In addition the customer shall comply with all relevant legislation that covers their specialist area of activity, such as, but not limited to, the Data Protection Act 1998, the Education Act 2011 and similar. At all times users should act in such a manner as to protect the confidentiality of the information being processed in accordance with the Data Protection Act 1998.

This Code of Connection Policy incorporates the main principles of relevant UK legislation with regards to use of IT systems and data. There is also a requirement for compliance with a variety of Code of Connections as a pre-condition for sharing information with government departments or other public bodies. The onus is on the customer to demonstrate and provide evidence of compliance for all of these regulations as they are published.

3 Responsibilities

3.1 Customer

The customer **shall** ensure the Code of Connection is implemented within their connected organisation. The customers AUP **shall** not be less restrictive than this Code of Connection.

3.2 Employees / users

All users **shall** familiarise themselves with the customer AUP. They **shall** adhere to the terms of this document when using ICT equipment, regardless of ownership, when connecting to the internet through the BLN.

3.3 Third Parties

The customer **shall** ensure that third parties, who use the customers ICT systems, are aware of the requirement to comply with the customer AUP. Contracts between customer and third parties **shall** reflect the requirement to comply with BLN Code of Connection when accessing resources.

4 Business use, personal use and misuse of ICT

4.1 Business Use

The BLN's internet facilities are a business resource provided to customers to be used by that customer for their business related purposes. The BLN **shall** not be resold or shared with other organisations without consultation and authorisation from the School Reference Group via the BLN Project Manager.

4.2 Personal Use

The BLN recognises that users, from time to time, may need to deal with private business or personal matters during the course of their working day. The BLN requires that each customer makes appropriate allowance for this type of use in their AUP but also ensures that they monitor the operation of their AUP such that any use does not overstep legal obligations a customer has with respect to its employees and ensures the BLN is not brought into disrepute.

4.3 Misuse

Misuse of ICT can cover any activity carried out using any ICT resources to access the BLN, for example:

A User **shall not**:-

- Use ICT systems for any purpose which would reflect negatively on the customer, BLN or its employees.
- Carry out any activity which would cause damage or disruption to BLN operations, or which would constitute a criminal offence.
- Create, transmit or disseminate material that may bring the BLN's name or the name of any of its employees into disrepute, whether on their own device or personal websites.
- Break or attempt to avoid or break through the customers and the BLN's security controls.
- Undertake any activities that violate laws or rights of third parties, e.g. installation or distribution of unlicensed software; unauthorised copying of copyrighted material; storage of such materials on any systems which will connect to or access the BLN.
- Use the BLN internet IDs, e-mail addresses, IP information and resources for anything other than authorised communications.
- Intentionally access, view or download pornography, or any type of illegal material or material which contravenes the establishments AUP and thus the BLN's Code of Connection.
- Access, retrieve, or print text and graphical information which exceeds the bounds of generally accepted standards of good taste and ethics or which contradicts the organisational values and/or employment policies thus putting the BLN into disrepute.
- Carry out any activities which would incur any unauthorised costs to the BLN.
- Enter into personal legal transactions which would bring the BLN into disrepute.
- Intentionally access, execute or transmit malicious software (e.g. viruses, worms, Trojan horses etc.).
- This list is not exhaustive, and the BLN reserves the right to take action against an establishment who, in the reasonable opinion of the BLN, has misused/abused the network.

4.4 General Controls

No user is permitted to remove equipment or connections from the BLN installed systems or use technical control measures to cut off its reception and transmission to and from the BLN without prior notification and agreement unless to prevent such issues as denial of service or viruses from affecting the BLN network.

Devices that contravene the BLN Code of Connection **shall** not be connected to any resources. The use of analysis tools on the BLN, and other actions which can influence or impair system stability and security, **shall** only be performed under the authorisation of the BLN.

Users **shall** notify their supervisor, manager or teacher of any abuse of software or accompanying documentation. The BLN **shall** be informed if the incident brings the BLN into disrepute.

There may be some circumstances where for valid operational reasons some of the practices listed above may be authorised by the establishment's senior manager without prior approval from the BLN for business continuity reasons. In these cases the senior manager responsible **shall** follow internal processes and ensure an audit log is completed and filed. BLN **shall** be informed of any such action taken together with a detailed justification.

5 Scanning and Monitoring

5.1 Content Scanning

Automated filtering systems are used as a means of protecting against viruses or other security threats, and of detecting inappropriate content. The automated systems maintain logs of inappropriate activity. The BLN **shall** provide the necessary legally required protection within the core network to prevent against such inappropriate content. Where the customer chooses not to take service from the BLN they **shall** ensure that the services they provide or alternately procure comply with all necessary legal protection. This will include but not be limited to alternate email services, virus protection and spam filtering. Customers **shall** be responsible for all appropriate protection of their internal network.

5.2 Monitoring

Some BLN systems are routinely monitored for performance and service i.e. internet connectivity to connected organisations, but specific website content (although scanned) may not be monitored routinely. Monitoring of bandwidth and content may be used to allow the BLN to evaluate use of systems. The results of this monitoring may be used to inform the customers disciplinary procedures where necessary, should the need arise, or to comply with a RIPA request.

6 Violations of the Policy

Where it is suspected or established that a user within a connected site is abusing or misusing the BLN, such abuse or misuse **shall** lead to the restriction or the withdrawal of any or all of the facilities for that customer until such time as the issue is resolved.

The customer AUP **shall** cover the user disciplinary procedure if there is a violation of the BLN Code of Connection. Violations of the Code of Connection could also amount to criminal offences and potentially lead to prosecution.

7 BLN Supplied ICT Equipment

ICT equipment which is provided by the BLN for business purposes remains the property of the BLN when installed in a customer's premises. This policy applies to all BLN ICT equipment which is not subsequently transferred to the school.

8 Super User Access to BLN ICT Systems

Some customers will have a requirement to have a "super" user who will have the ability to make changes to policies on behalf of the whole connected organisation. This will be via the BLN ICT systems and information is provided on the basis that users are given a level of access required to enable them to carry out the work they are authorised to do. This access **shall** be controlled through the use of user accounts and passwords for all super users. Levels of access to ICT systems and information **shall** be limited to the role and activities that the user has been authorised to do.

8.1 General Rules

- Access to each BLN ICT system **shall** be managed by Specific User Identifiers (User IDs) and Passwords
- Access to BLN business software applications and user access maintenance are the responsibility of the BLN Team who will work in conjunction with the customer
- Systems owners or ICT support **should** define and log which levels of access to the internet are authorised to which groups of users
- There **should** be procedures in place to regularly review user access to BLN related resources and to ensure that user's who no longer require access, are removed
- Users **shall** keep passwords confidential and **shall** adhere to any BLN related password policies when accessing BLN related resources (where applicable)
- Users **should** change passwords regularly
- Adhere to the password policy of the connected organisation

Shall not:-

- Disclose any BLN related passwords to anyone
- Share an internet user identifier and password with anyone else. It is a personal identifier and the individual **shall** be held responsible for all internet access related actions undertaken by that unique user identifier
- Save internet access related user names and passwords in web browsers or other caching systems

9 Virus Protection

The BLN has ensured that on all BLN ICT systems (where necessary), continuous protection is enabled by approved virus scanning software with a current and updated virus application. In order to minimise the risk of viruses entering the BLN's ICT systems, users must not load unauthorised software onto any ICT systems or download software from the internet which may cause harm to any BLN ICT systems. Customers **shall** ensure all their internal ICT systems are fully protected against virus attacks, and that this protection is updated at least daily.

Generally, more damage to files can be caused by inappropriate corrective action than by viruses themselves. Any incidents must be reported immediately to the customer ICT service or designated provider. If a virus is suspected, once reported, the customer **shall** take necessary steps to ensure the virus is restricted to the one device, disconnecting their network from the BLN if necessary.

10 Information relating to or used on the BLN

10.1 Intellectual Property and Copyright

- Where a user has access to or has received information relating to BLN systems then they **shall** surrender all related information on leaving their employment. No information relating to the BLN may be retained for personal use. Customers **shall** ensure that their internal contracts with employees cover the surrendering of information relating to your systems.
- Users **shall not** use within the BLN any material that they either know, or suspect to be, in breach of copyright.
- Users **shall not** pass such material on to anyone else to use on the BLN.
- Users **shall** appreciate that information offered on the internet is protected by property rights and consequently **shall** work to ensure that this information is accessed or used appropriately in recognition of these rights.

10.2 Non- Disclosure

BLN related information of a personal, confidential or commercially sensitive nature **shall not** be disclosed to anyone unless authorised in writing by an appropriate BLN Officer. Information must be treated as a valuable asset and handled accordingly.

10.3 Use of Information Accessed

Users that have access to sensitive or personal information from any source through the BLN resources, **shall** only use the information gained for its intended purpose and not bring the BLN into disrepute. Violation of this principle **shall** breach the terms of this code of connection but may also breach Data Protection legislation which protects confidentiality. Violation of either or both could constitute gross misconduct.

10.4 Information Published on the Internet

BLN related information published on the internet, websites, blogs, social networking sites or on any other publicly accessible media, must be authorised by a designated person within a connected organisation prior to publication.

11 Using E-mail Facilities

E-mail provides users with a speedy, convenient and efficient means to communicate information. Where a customer chooses to use the BLN related email service, then the below rules should be adhered to.

A user **shall:**-

- Manage e-mail to ensure use does not exceed relevant e-mail capacity.
- Report inappropriate use or content to a customer designated officer in the first instance and in line with the customers AUP.
- Delete any suspicious messages received from unknown sources.

A user **shall not**:-

- Send messages using another user's accounts unless appropriately authorised to do so e.g. "sent on behalf of".

- Forward an e-mail from an address or person not recognised.
- Use language which might cause offence or be seen as abusive or discriminatory,
- Send or forward jokes, chain letters or other offensive or inappropriate content.
- Send files or documents from a computer that does not have up to date anti-virus and malware protection.
- Give out personal information or confidential information unless appropriately authorised to do so.
- Use a work related email address to conduct personal business activities.
- This list is not exhaustive, and the BLN reserves the right to take action against a user who, in the reasonable opinion of the BLN, has abused the system.

11.1 Mailbox Access

Users **should** be aware that access can be provided to their individual mailboxes in relation to business activities in their absence or as a result of the termination of their employment from the connected organisation. Permission **shall** be sought from an appropriate senior manager via the BLN change request process for such activities.

11.2 Sensitive Information

The privacy and confidentiality of messages sent via e-mail cannot be guaranteed. Users are advised that all external e-mails have a disclaimer at the footer of the e-mail to protect the establishment and the BLN from information being disclosed to unauthorised personnel. However, there is no guarantee that this will protect individual personnel from potential legal action if e-mails sent include unsupported allegations, sensitive or inappropriate information. It is the responsibility of all users to exercise their judgement about the appropriateness of using e-mails when dealing with sensitive subjects. When sending sensitive information by e-mail, an appropriate protection method must be employed to ensure the security of the information. It is down to the customer to show they are conforming to this practise.

The above rules **should** also be taken into consideration and applied as best practise to any AUP, where a customer has either their own hosted email service or is contracted into a third party email service

12 Using the Internet

The internet provides a valuable source of information for the customer and its users. The BLN recognises the value of the internet as a source for information for teaching and learning and as an excellent means of communicating quickly to a wide audience. At the same time the internet is largely unregulated and it must be used advisedly. It can be a source of security threats, and information available from it may not be reliable, up-to date or accurate. It is to be used in a manner that is consistent with the BLN's and customer values and standards of business conduct, and as part of the normal execution of job responsibilities.

12.1 Accessing the internet

To ensure maximum security and avoid the spread of viruses, Users accessing resources using the BLN **shall** do so through an approved Internet firewall or other security device. Bypassing and gaining access to the internet or other networks directly whilst on school premises using any ICT equipment (whether belonging to the customer or personal) through the BLN is strictly prohibited.

12.2 Frivolous Use of the Internet

Computer resources are not unlimited. Network bandwidth and storage capacity have limits, and all users connected to the network have a responsibility to conserve these resources. As such, the customer **shall not** deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others including but not limited to creating unnecessary loads on network traffic associated with non core business related uses of the Internet.

Where a customer has been identified as misusing internet resources to the detriment to other customers, the BLN reserves the right to take action to remedy this which may involve isolating and/ or disconnecting/ limiting the use of the internet for that customer until the issue has been resolved.

12.3 Use of BLN Internet Facilities

A User **shall**:-

- Exercise caution when surfing unfamiliar or untrusted websites
- Be specific in the use of words when using search engines
- On inadvertently discovering a website which contains any material which could be judged to contain sexually explicit, racist, violent or any other potentially offensive material, disconnect from the site immediately. Report this event to a customer designated reporting officer
- Report anything suspicious to your customer designated reporting officer

12.4 Blocked Websites

Through the application of BLN content filtering, the BLN **shall** restrict/bar websites based on IWF guidelines. Customers choosing not to use the BLN recommended filtering system **shall** ensure that they are adhering to IWF guidelines. Where websites have been blacklisted they **shall** not be unblocked unless there is a valid business or educational requirement for this. Each customer has been provided with means to edit their own website allow/deny list in accordance with their AUP. An internal audit trail **should** be put in place to manage this process. Requests for access to globally blocked websites will require BLN service authorisation.

12.5 General Website Browsing

Whilst adhering to the BLN's Code of Connection the general rules of browsing legal and educational related content on the internet through BLN related resources **shall** be governed by the customer AUP. Outside of the IWF related governance, the block/allow list for each school **shall** not fall under the scope of this Code of Connection but the customer **shall** ensure that the BLN is not bought in disrepute.

12.6 Information Reliability

All information on the internet **should** be considered suspect and valued accordingly when used in the school's teaching and learning processes. Only use information provided by sites which you trust and have checked prior to sharing or using.

12.7 Copyright

Upload or download of materials **shall** be within the confines of copyright law. Users **shall not** upload, download, or otherwise transmit commercial software or any copyrighted or suspected copyrighted materials belonging to parties outside of the connected organisation, or the BLN itself. Download of media files such as music and video (e.g. mp3, mpeg, avi, etc) files is prohibited unless within copyright law. If in doubt, advice **shall** be sought from the connected organisations designated member of staff.

12.8 Protection for you

The person identified as using the internet will be considered to be the person using it. For this reason users **shall** always log out or lock a computer when not using it. The customer **shall** be responsible for identifying a user if such information is required by, for example, a RIPA request. The BLN team **shall** assist with this function where they have access to this information and that information has not subsequently been denied to it by blockages put in place within a designated connection.

12.9 Guest Access to the Internet

The customer **shall** accept full responsibility for all users and will take responsibility to ensure the user signs their customer AUP and adheres to all policies related to this. The user **should** sign in with a specific identifiable login account to access the internet.

13 Security Incidents

Users **shall** immediately report to their locally designated person when:-

- Information in any form which can/may bring the BLN into disrepute has, or is suspected to have been lost or disclosed to unauthorised parties.
- Unauthorised use of the school's information systems has taken place, or is suspected of taking place thus resulting in defamation of the BLN.
- Passwords or other systems access control mechanisms are, or are suspected of having been lost, stolen, or disclosed which may cause a breach of BLN services.
- The BLN ICT Service **shall** be immediately contacted about unusual BLN related systems behaviour and frequent BLN system crashes.
- Service managers or IT support, on being notified of a potential security incident, **shall** agree the appropriate course of action to be taken with the Senior Manager of the connected organisation.
- Details of security incidents or suspected security incidents **shall** be treated as "Confidential" and only discussed with those parties engaged in the connected organisation and/or BLN's investigation process.

- When a security incident is suspected it is very important to report it as quickly as possible. The earlier an incident can be identified and its impact assessed the greater the chance of dealing with it successfully.
- All breaches of the customer AUP **shall** be reported in line with the requirements of that customer AUP.
- If a user suspects that another user is abusing or misusing BLN related systems they **should**, in the first instance, contact the designated senior manager.
- If a user suspects that a supervisor or manager may be associated with misuse or abuse then such concern **should** be reported to the next senior manager for their attention. In extreme cases such concern can be reported direct to the BLN who will use the services of the Council to investigate appropriately.
- A response to serious concerns about illegal conduct or behaviour, **should**, in the first instance be reported in accordance with the customer AUP. In extreme circumstances a user may report such concern direct to the BLN where appropriate action will be taken.
- Where the BLN recognise that such misuse may cause harm or disruption to other customers or the BLN, then it reserves the right to isolate or disconnect the establishment concerned without prior notice or discussion until such time as the issue has been resolved.