



Policy Documentation:
ICT User Policy

(v2.4)

DOCUMENT PURPOSE:

This ICT User Policy applies to all computer users working for, or on behalf of, the Coal Authority; this means anyone who is authorised to use and/or access our computers, IT infrastructure, computer software, information and data.

Signed acceptance of this policy must be provided prior to being granted access to any Coal Authority ICT systems or devices.



Contents:

1.0	About the ICT User Policy.....	3
2.0	Access to Systems.....	4
3.0	Responsibility for Accounts.....	5
4.0	Authority Equipment & Network Infrastructure	6
5.0	Data Storage, Handling & Processing.....	7
5.1	Confidentiality.....	7
5.2	Document Change Tracking	8
5.3	Data Aggregation.....	8
6.0	Network Security and Computer Viruses.	9
6.1	Virus Alert Procedure:.....	9
6.2	What you MUST do to protect against viruses:	9
6.3	What you must NOT do:	10
7.0	Procurement.	11
8.0	Email.....	12
8.1	E-mail Style & Size	12
8.2	Bulk Mailing	12
8.3	Personal Use of E-mail	13
8.4	Unacceptable Use of E-mail.....	13
8.5	E-mail Security Considerations.	14
9.0	Internet Access.	15
9.1	Personal Internet Usage	15
9.2	Unacceptable Internet Usage.....	16
10.0	Guidance on Handling Personal Data in the Computer System and Disclosure of Documents in Legal Proceedings	17
11.0	Monitoring of ICT, Internet and Email Use.....	19
12.0	Incident Reporting.....	22
	Appendix A – Sign Off Sheet	23
	DOCUMENT CONTROL:.....	25



1.0 About the ICT User Policy.

This policy applies to all computer users working within the Coal Authority, which means anyone who is authorised to use and/or access our computers, IT infrastructure, computer software, information and data.

It is the responsibility of all staff to ensure compliance with this policy in full and without exception and report any breaches or suspected breaches to a Senior ICT Manager, the Head of ICT or the Head of HR&OD.

Contravention of this policy could lead to disciplinary action for Authority staff, or a report to the employers of third party staff working on site, requesting that such action be taken.

I confirm that I have read and understand my responsibilities outlined in

Section 1.0, "About the ICT User Policy"

please tick **[x]**



2.0 Access to Systems.

All computer users are permitted access only to those parts of computer systems that they have been given permission to access and need to do so in order to carry out their normal duties. Any other access will be regarded as unauthorised.

Should a computer user believe that they need to gain access to other parts of the Authority's computer systems, this should be requested via the Authority's formal [change request system via the Intranet](#) and approved by their Line Manager in the first instance. Alternatively, authorisation must be provided from the Senior I.T. & I.A Manager or Head of ICT.

Only users with a named account may gain access to internet and e-mail services.

<p>I confirm that I have read and understand my responsibilities outlined in Section 2.0, "Access to Systems"</p> <p style="text-align: right;"><i>please tick</i> [x]</p>
--



3.0 Responsibility for Accounts.

All Authority computer users will be issued with a user account and password used to uniquely identify them. Computer users may only access Authority computer resources using the account name and password allocated to them. Use of IT resources is restricted to registered members of Authority staff or approved, supporting third parties.

You are directly responsible for your own account. Any and all actions performed using an account, are the sole responsibility of the account holder. Anything that happens on the Authority's computers under your username is your responsibility.

You are expected to take all reasonable precautions to prevent unauthorised use of your account by another person. This includes, but is not limited to, safe-guarding your username and password, ensuring that you correctly log off your account and lock your screen when away from your computer or desk.

You will be provided with a password. This is confidential and should not be disclosed to anyone - whether or not that person works for us. The password should be changed whenever prompted by the system.

You must also comply with any rules or requests covering network security issued by the ICT department.

I confirm that I have read and understand my responsibilities outlined in

Section 3.0, "Responsibility of Accounts"

please tick **[x]**



4.0 Authority Equipment & Network Infrastructure

All Authority users will be provided with the required computer equipment, configured in accordance with ICT specifications, to undertake their daily duties. Where a user believes they need access to other computer equipment or resources they should contact the ICT team or their line manager for approval.

Members of staff are strictly forbidden from:

- Attempting to use Authority computer equipment which has not been assigned to them for use in their daily duties by the ICT team or line manager.
- Attempting to move, open, upgrade or modify any Authority computer equipment.
- Attempting to re-patch data or voice network connections.
- Attempting to alter the configuration of software on their computer (including the installation of software).
- Attempting to bypass software security settings or identification and authorisation procedures.
- Attempting to bypass security software and operating system settings.
- Connecting non-Authority provided equipment including (but not limited to):
 - Portable Hard Disk Drives (HDD's)
 - Personal phones, smart phones, PDA's, MP3 players

Such devices are strictly forbidden from being connected to the Authority's network, or other resources in any form.

ANY external storage device (including those devices listed above) that needs to be accessed from Authority laptop/desktop computers must first be scanned for virus infection using the "sheep dip" computer in the print room.

Coal Authority issued smartphones and tablets **must** be anti-virus scanned using the Authority sheep dip computer, **after** connecting to your own PC and **prior** to connecting to an Authority laptop. Please see the mobile iphone/ipad user policy for more details.

Please contact ICT if a virus alert is displayed during the scanning process.

<p>I confirm that I have read and understand my responsibilities outlined in Section 4.0, "Authority Equipment and Network Infrastructure" <i>please tick</i> [X]</p>
--



5.0 Data Storage, Handling & Processing.

It is critical that all permanent data is managed correctly. Therefore all permanent data created or processed during your daily duties must be saved to network drives and not local drives (ie: C: and D:) on your PC or laptop. This will ensure that the data is backed up according to the Authority's backup policy.

Where information is of a secure or confidential nature, appropriate security should be applied by the member of staff to prevent unauthorised access. This means saving any such content into a suitable area of Wisdom (or the network) that has suitable access control policies applied. Please consult your line manager or ICT if you are in any doubt about the classification of the information you are working with or where to save your documents.

Local drives may only be used for the temporary storage of transient data. Staff should be aware that ICT are unable to backup and therefore recover any data held locally on a user machine, significantly increasing the probability of data loss where such data is stored.

Where data needs to be shared within a team, or with other teams, it should be placed in the appropriate network drive or Wisdom folder.

All users are provided with a secure personal network drive (N:). Personal drives are limited to 100Mb in size and should be used to store only personal Authority information such as training plans, performance management information, etc.

Network drives and personal drives must not be used for storing non-work related, personal information – including, but not limited to, photographs, letters, media files etc.

5.1 Confidentiality

Any sensitive (personal or commercial) Authority data must be held securely and in accordance with its handling instructions, and must not be shared by any means to an outside party, unless prior permission has been granted by the relevant information asset owner (IAO) and/or by an IAO approved process.

Where data is of a sensitive or confidential nature, or may be subject to the Data Protection Act (whether it may be stored digitally or physically), staff must seek advice from your [departmental information asset owner](#), line manager or the Information Assurance and Business Continuity Manager regarding the most suitable method and location for storage of that data within the Authority's ICT systems.



5.2 Document Change Tracking

Document change tracking (MS Word 'Track Changes') must not be used in any documents which may contain sensitive or confidential information. Failure to remove tracked changes may allow a recipient to obtain confidential or sensitive information by examining the tracked change history created during the documents life.

Where possible, any documents with sensitive information should be converted to PDF and signed before sending out to recipients.

Where you believe that you have confidential or sensitive documents with tracked changes, please contact the ICT service desk who can assist in their removal.

5.3 Data Aggregation

When storing, processing or sharing/transmitting data, staff must consider the impact of data aggregation (ie: combining data sets which originated from a number of sources). Data which may not have been considered confidential or sensitive alone, may well have implications for information handling when combined with other data sources. This issue may occur where several data sources are included in a single message or document, or several communications are sent to an individual or organisation.

Staff must consider the consequences of data aggregation over the life of the data and ensure it is handled in an appropriate manner when:

- handling, storing, processing and transmitting data;
- dealing with an external person;
- dealing with an external department or organisation;
- dealing with any group, body or organisations who may be in contact with each other;

If you are in any doubt about the implications of storing, processing or transmitting any aggregated data sets you are working with, you should consult your line manager in the first instance and/or review the [Authority's IRM Policy](#).

I confirm that I have read and understand my responsibilities outlined in Section 5.0, "Data Storage, Handling and Processing" <i>please tick [X]</i>



6.0 Network Security and Computer Viruses.


A computer virus is essentially a piece of computer software or a program designed to replicate itself from computer to computer without participation of the computer user. Once loaded into a computer, it can cause loss of data and software on that computer or network. Sources of viruses include the internet, USB storage devices, e-mail messages, software, and removable media introduced into the Authority via a route other than the ICT Department.

All Authority computers have anti-virus software installed whose status is monitored daily.

You must not attempt to disable, remove or otherwise interfere with this software in any way.

6.1 Virus Alert Procedure:

If you suspect your computer has a virus, switch it off immediately (press and hold the on/off button) and...



Contact a member of ICT immediately if you receive a virus alert notification:

T: 01623 637 400	(ICT Service Desk)
T: 01623 637 315 / 380	(ICT Desktop Support)
T: 01623 637 267 / 220	(Senior ICT Manager)

6.2 What you MUST do to protect against viruses:

- Virus scan all media from any outside source for viruses. The virus scanning station (aka: “sheep dip”) has been located in the MIC print room, is clearly marked with scanning instructions on the Windows desktop.

Please contact the ICT Service Desk for any assistance.

- If you receive a virus alert on your work computer, power your machine down immediately and contact the ICT support team. Do NOT shutdown as normal. Press and hold the on/off button (laptops/desktops).
- If you receive an e-mail message informing you that an attachment has been removed or quarantined by the system because of a possible virus. You must



contact the ICT support team immediately for advice, do NOT reply to the sender.

- Be vigilant and assist the ICT Department both generally and when spot checks are carried out as part of the security procedures put in place to protect our data.
- Comply with any rules issued by the ICT Department covering remote access to the computer network.

6.3 What you must NOT do:

- Run or load unauthorised software on any equipment provided to you by the Authority, including software downloaded from the internet. This also extends to the use of illegal, copyright infringed and/or otherwise inappropriate media files which may cause offence
- Follow any instructions you receive on an e-mail message informing you that there is a virus on your system. These messages are usually hoaxes or viruses themselves. Inform ICT support immediately.
- Accept copies of software from others. If you have a legitimate need for the software you are being offered, then contact the ICT Department to either purchase it for you, or to check it thoroughly before it is loaded onto our systems.
- Access unauthorised areas, applications, data or websites.
- Install, replace, bypass, or modify any security feature that would render our information insecure or prevent us from monitoring the use of our systems.
- Copy or distribute to any third party company, Authority software or data.

<p>I confirm that I have read and understand my responsibilities outlined in Section 6.0, “Network Security and Computer Viruses”</p>	<p><i>please tick</i> [x]</p>
--	--------------------------------------



7.0 Procurement.

All IT equipment and software for use within the Authority must be purchased through the ICT Department. It is not permitted for any member of staff to purchase equipment or software directly for use within the Authority without the express permission of the Head of ICT. For details on the ICT purchasing process please contact the ICT team for advice or [complete a request for change](#).

Please note that the ICT team reserve the right to remove, and/or refuse technical support for, hardware/software that is not purchased in accordance with these guidelines, or that has not been recommended or approved by the Authority's ICT Department.

I confirm that I have read and understand my responsibilities outlined in

Section 7.0, "Procurement"

please tick [x]



8.0 Email.

The Authority provides all registered computer users with an e-mail account for use in connection with the Authority's business. Staff may only send e-mail from their registered account. Use of another person's e-mail account, with or without permission, is not permitted. Personal use of e-mail is permitted provided it does not interfere with that business or otherwise contravene this policy.

Staff should be aware that when an e-mail is sent, or is likely to be forwarded outside of the Authority, then its contents will also be subject to the acceptable use policy of the ISP. Details are available on request from ICT.

8.1 E-mail Style & Size

All communications by e-mail are identifiable as originating from the Authority and must be treated as if they are permanent written communications from the Authority; an appropriate language and style should therefore be used at all times.

Staff should be aware that in common with most e-mail systems, the Authority's mail system is unable to handle e-mails which exceed 25Mb in size. Where an e-mails size exceeds this threshold, suitable compression software may be utilised or an alternative delivery mechanism agreed.

If you need to transmit large files outside of the Authority please review the [IRM Policy](#) (or your Line Manager) for any necessary Information Handling considerations and consult ICT for guidance

8.2 Bulk Mailing

The Authority's e-mail system may not be used for the bulk mailing of messages without prior permission from a Senior ICT Manager or Head of ICT. Bulk mailing is considered to be more than fifty recipients of the same message (which applies whether the message is sent to more than fifty addresses individually or a single message with more than fifty addresses in the recipient list).

To help avoid breaching Data Protection Act (DPA) regulations, the BCC (blind carbon copy) field must be used if your recipients are non-Coal Authority staff or they have not explicitly consented to their email addresses being shared with the distribution list in question. The ICT Service Desk can provide guidance on the use of externally hosted mail services to facilitate emailing a large number of external recipients and avoid DPA breaches.



Even if your bulk e-mail is legitimate, email messages should never be sent to more than 499 recipients in one batch. Failure to follow this policy may result in the Authority's mail system being externally blocked, severely impacting the Authority's business.

8.3 Personal Use of E-mail

Whilst it is accepted that you may send and receive limited personal communications by e-mail, these should be minimal and the privilege not abused, just as in the case of personal telephone calls. You must ensure that any private use does not interfere with the performance of your duties and should preferably be conducted:

- Before your normal work time commences.
- During your lunch break.
- After your normal finish time.

Please note that technical support from the ICT department will only be provided for Authority e-mail accounts, and not for any personal mail accounts.

8.4 Unacceptable Use of E-mail

There are certain types of communication which could give rise to liability both for yourself and potentially for the Authority. For this reason, you must NOT send or (where preventable) receive, any personal or business e-mail that:

- Contains pornographic, obscene, defamatory, discriminatory or insulting material, whether or not you are offended personally by it;
- Contains information that is confidential, personal, commercially or client sensitive, or may have contractual or other legal implications for us, except as part of your duties;
- May be deemed as 'junk mail', such as jokes, stories or chain letters;
- May damage our reputation or that of any person or organisation with which we deal;
- Includes derogatory remarks about other people or organisations (even if only sent internally);



- Makes representations or expresses opinions purporting to be ours, except where authorised;
- May constitute sexual, racial or other harassment.
- Contains links or instructions which would direct a recipient to material of the nature outlined in the points above.

You are expressly warned that e-mail messages can be recreated even after deletion and may be used in legal proceedings.

8.5 E-mail Security Considerations.

Email should not be used for the distribution of sensitive business information outside of the Authority.

Staff are reminded that that e-mails are not secure, may be intercepted, delivery may be unreliable, and you should be aware that this is outside of the Authority's control.

Therefore, do not rely on e-mail for time sensitive or commercially confidential material. E-mail should be thought of as "best effort" and not guaranteed delivery. The same rules apply for incoming e-mails.

For sensitive material such as personal details we would recommend that more secure, physical methods of delivery be considered, such as post or courier where the recipient must sign acceptance of the delivery.

I confirm that I have read and understand my responsibilities outlined in

Section 8.0, "Email"

please tick **[x]**



9.0 Internet Access.

Internet use to support activity connected with the Authority's business, including client, and/or customer communication, research, administration and the development of professional knowledge is not restricted.

Where staff are using the internet to access hosted services provided by another organisation, they may only do so with the express permission of the Authority's Senior I.T./I.A. Manager or Head of ICT, and with the hosting organisation's relevant Authority. Where deemed necessary, it may be required for the person to request evidence of these permissions. ICT authorisation can be sought by [completing a request for change](#).

9.1 Personal Internet Usage

As in the case of e-mail, the Authority recognise that certain employees will have a legitimate business need to access the internet, and also that a reasonable and minimal amount of access for personal purposes is acceptable.

Internet use for personal purposes is allowed provided it is minimal, reasonable and does not interfere with the performance of your duties. The Authority reserves the right to restrict access to certain categories of website, eg webmail or file sharing.

These activities should preferably be conducted:

- Before your normal work time commences
- During your lunch break, or
- After your normal finish time

Staff are reminded that a record of internet browsing and email activity may be monitored, archived and reported on. [See section 11.0 of this policy for further details](#).

Please note that technical support from the ICT Department will only be provided for websites accessed that are specifically connected to Company business. The ICT Department will not provide support or accept any liability for external websites that are accessed for personal use, such as websites that require you to enter credit card and/or other personal details. We strongly advise you against accessing such sites.



9.2 Unacceptable Internet Usage

There are certain types of internet usage which could give rise to liability both for yourself and potentially for us and result in a criminal offence being committed. For this reason, you must NOT utilise the internet for the following activities:

- use of our internet facilities to access, view, download, print or distribute pornographic, indecent, sexually explicit, obscene or copyrighted material or material likely to cause offence, whether or not this would constitute a criminal offence and irrespective of whether you do so during working hours or whether you personally find such material insulting or distasteful is strictly prohibited;
- playing computer games, online gaming, misuse of video files, private advertising and use of the internet for personal financial gain is also strictly prohibited;
- no member of staff is permitted to publish or moderate material via the internet either on a web site, ftp, bulletin board, newsgroup or message board without the prior permission of the ICT manager;
- no member of staff is permitted to download image, audio or video material in any format which does not directly correspond to their daily duties for the Authority;
- no member of staff is permitted to utilise their Authority e-mail address to sign up to personal interest web sites, services or automated e-mail alert services which do not directly correspond to their daily duties for the Authority;

You may inadvertently access inappropriate material because of misleading site descriptions or innocent searches. If this should happen you should exit the site immediately. Failure to do so with due speed may result in us concluding that you deliberately viewed the material.

The Authority reserves the right to remove internet access from any individual without prior notice.

**I confirm that I have read and understand my responsibilities outlined in
Section 9.0, "Internet Access"**

please tick [X]



10.0 Guidance on Handling Personal Data in the Computer System and Disclosure of Documents in Legal Proceedings

With the increasing proliferation in the methods in which we can receive and create electronic information we all need to be increasingly mindful of our legal obligations when creating, storing or circulating information, particularly when this is in regard to individuals. Information relating to any identifiable individual which is created on the Authority's computer systems (e.g. a word document or e-mail) counts as "personal data" for the purposes of the Data Protection Act 1998. (DPA)

Once we hold personal data about an individual, we have obligations relating to that data. We must ensure that the data is accurate, not excessive or irrelevant and we can "process" the data only if strict conditions are satisfied. In brief, most data can be processed for legitimate business reasons but there are additional limitations on the processing of sensitive information (e.g. about an individual's health). Circulating, retaining and even deleting information counts as processing.

Individuals have a right, subject to certain exceptions, to see personal data that is held about them on the Authority's computer system. We may also have to disclose documents, including e-mails, in the context of legal proceedings (whether or not they count as personal data). If you wish to make a subject access request under the data protection act, you may send your written request to the **Data Protection Officer**, The Coal Authority, 200 Lichfield Lane, Mansfield, Nottinghamshire. NG18 4RG.

Please note that we reserve the right to charge an administration fee for obtaining and sending this information to you. We may also require you to confirm your identity to us to ensure that we are releasing your private information to you. This may require you to personally meet with the Data Protection Officer, or a representative of the HR team, to verify your identity. Any information we release to you under our DPA obligations is for your personal use only and must not be published, reproduced, broadcast or distributed in any way without our prior written permission of the Data Protection Officer.

Against that background, here is some practical guidance on handling information about individuals held on computer:

- Beware what you say in e-mail messages. If sending an e-mail about an individual, remember that this is likely to be processing personal data. This means that the individual may seek access to it and we have data protection obligations in respect of it. Consider whether a telephone call would be a more appropriate means of communicating the information.



Remember that describing an individual by their initials (“ABC”) or indirectly (“you know who”) will often still count as processing data about the individual.

Never ask for or send information about someone’s health or other sensitive details unless they have specifically agreed to this or you know that you are acting within the limits of the Data Protection Act.

- Never make “throw-away” remarks about individuals in e-mails, assuming that they won’t see them.

Subject access requests are becoming more common and this sort of remark can lead to legal liability. Remember that e-mails are not a secure method of communication and can be forwarded very easily to individuals other than the intended recipients both deliberately and by mistake.

**I confirm that I have read and understand my responsibilities outlined in
Section 10.0, “Guidance on Handling Personal Data in the Computer System and
Disclosure of Documents in Legal Proceedings”** *please tick* **[X]**



11.0 Monitoring of ICT, Internet and Email Use.

All internet usage is logged automatically by the Authority's systems for security purposes. The source and destination of connection, time and number of bytes transferred are all logged and these details are kept for up to six months before deletion. We periodically review a list of sites accessed by users to identify any inappropriate sites which might have been accessed.

All e-mail is content-filtered both coming in and going out of our network. This is carried out on an automatic and continuous basis. If any e-mail fails to meet the requirements it is quarantined into either the junk mail or spam mail folders. Occasionally, genuine e-mails will be filtered into these folders. Messages classified as spam will be quarantined, and you will receive a daily "Message Manager" email detailing which messages have been withheld and how to release them if they have been incorrectly withheld. You are therefore advised to check your Message Manager e-mail immediately upon receipt and your spam mail folders periodically.

Occasionally, a genuine e-mail will be incorrectly quarantined as containing offensive material. Staff will not be notified when this occurs. You are therefore advised to contact ICT if believe you should have received an email which may have been incorrectly quarantined.

If the title of an e-mail arriving on our server or the content of an attachment to a mail checked by the ICT Department, alerts the ICT Department to a breach of this policy, or other inappropriate behaviour, they will notify the HR Department or a Line Manager accordingly.

We may also monitor your e-mails and internet usage:

- Where a breach of this policy, a breach of another policy, or other inappropriate behaviour is suspected.
- To check for viruses.
- To check facts or control quality.
- If a member of staff is absent and e-mails need to be checked for work-related reasons.

In order to monitor when a breach of a policy or other inappropriate behaviour is suspected or where facts or quality are being checked, we may open e-mails sent or received by you including stored or deleted ones.

The proactive monitoring and checking of ICT, internet and e-mail usage will be conducted by the ICT Department in conjunction with the HR Department or an appropriate Senior



Manager. It must only be authorised by the Head of ICT, Head of HR or other, appropriate Senior Manager.

Before authorising monitoring, the relevant manager will consider whether or not an alternative method of achieving the employer's objective might be used which is less intrusive.

You should note that marking e-mails as 'personal' does not mean that we will not, in some circumstances, see their content or attachments. If you do not wish us to read private e-mails you should make alternative arrangements that do not involve the use of the Authority's property or facilities. If you wish to communicate confidential information which you would not want monitored, for example, information about your or any person's health, consider using other means such as post, or confidential internal mail or by handing over the information in person.

We may override any passwords or require computer users to disclose any passwords in order to facilitate access to any e-mail message for a reason set out above.

Consequences of breach of this policy or failure to comply with any aspect of this policy without good reason could result in the removal of privileges to use the computer system for personal purposes and/or:

- In the case of employees, in disciplinary action being taken (including dismissal); in accordance with the Authority's disciplinary procedure as detailed in The Staff Handbook.
- In the case of non-employees, termination of the contract/relationship and/or legal proceedings.

The following will be regarded as gross misconduct and may lead to immediate dismissal of employees in accordance with the Authority's disciplinary procedure as detailed in The Staff Handbook; or, in the case of non-employees, immediate termination of the contract/relationship:

- Serious breach of our virus policy.
- Sending an e-mail which may materially damage our reputation or that of any person or organisation with which we deal.
- Sending an e-mail which constitutes sexual, racial or other harassment (whether or not it would be unlawful) or a breach of our harassment and bullying policy.



- Deliberately using our equipment to access internet facilities to view, download, print or distribute pornographic, indecent, sexually explicit or obscene material or material likely to cause offence.

You are specifically warned that there are a number of criminal offences that may arise from the misuse of our computer systems. The Authority reserves the right to inform the Police if we believe that such an offence may have been committed.

I confirm that I have read and understand my responsibilities outlined in

Section 11.0, "Monitoring of ICT, Internet and Email Use"

please tick **[X]**



12.0 Incident Reporting.

Any employee who identifies a breach of the Coal Authority's ICT User Policy should refer immediately to their Line Manager, a Senior ICT Manager or Head of ICT.

I confirm that I have read and understand my responsibilities outlined in

Section 12.0, "Incident Reporting"

please tick **[x]**



Appendix A – Sign Off Sheet

This sign off sheet relates to the Coal Authority's ICT User Policy, dated 03 December 2019. A copy of [this policy is available on the staff intranet](#) for you to refer to.

Should you have any enquiries relating to this policy please contact the Senior I.T. & I.A. Manager on 01623 637 267

This form must be signed and returned to the ICT Service Management team in order to receive your login credentials and before you start to use any Authority computer systems.

We recommend that you keep a copy of this document in an easily accessible location for reference.

I acknowledge receipt of and agree to comply with the document entitled: The Coal Authority ICT User Policy

Signature  Date ...3/12/2019.....

Print Name (Block Capitals)MYLENE RECEVEUR.....



Contacting the ICT Team: Suspected Virus Infections



Contact a member of ICT if you receive a virus alert notification:

- **Immediately power off your laptop or desktop then call...**

T: 01623 637 400 (ICT Service Desk)
T: 01623 637 315 / 380 (ICT Desktop Support)
T: 01623 637 267 / 220 / 231 (Senior ICT Manager)

Computer Usage Policy Breach



If you think believe that there has been a breach of this policy please contact one of the following Authority staff on the following numbers:

T: 01632 637 267 / 220 (Senior ICT Manager)
T: 01623 637 324 (Head of ICT)
T: 01623 637 311 (Head of HR)



DOCUMENT CONTROL:

Document Title: New ICT User Policy 030613

Current Version: v2.4

Author/ Owner: Matt Thorpe

Wisdom Ref: 003229845

Approved By:

Name	Role/Responsibility	Date
Paul Frammingham	Director of Finance & Corporate Services	12 Sep 2016

Reviewed By:

Name	Role/Responsibility	Date
Dan Whitt	Senior ICT Manager	12 Sep 2016
Matt Thorpe	Head of ICT	12 Sep 2016

Document Authors:

Name	Role/Responsibility	Date
Ragnar Karlsson	Information Assurance & Business Continuity Manager	12 Sep 2016

Change History:

Author(s)	Change Commentary	Version	Date
Ragnar Karlsson	Final version agreed for sign-off by Audit Committee	2.4	12 Sep 2016



Author(s)	Change Commentary	Version	Date
Ragnar Karlsson	Minor edits to ensure currency.	2.3	27 Jul 2016
Dan Whitt	Updated section 4 to reflect new DLP processes	2.2	16 Oct 2015
Dan Whitt	Minor edits and updates to section 5.1 and 11 to align with Ilias version	2.1	03 Sep 2015
Dan Whitt	Final version agreed for sign-off by Audit Committee and PJF	2.0	20 Jun 2013
Dan Whitt	2013 revisions and issued for stakeholder feedback.	1.2	04 Jun 2013
Matt Thorpe	Draft new policy	1.1	01 May 2012