Ixion

Ixion Group Policy & Procedure

e-Safety

for Learners, Customers and Ixion Staff

Policy Statement

The Ixion Group (Ixion) seeks to promote responsible use of technology for the purposes of training and development of staff, delivering services, employer engagement, and to encourage learners and customers to use digital communication responsibly. This policy encompasses the use of the internet, email, electronic communication and mobile devices.

Ixion provides customers with access to the internet and email through networked computers in our centres to conduct research, jobsearch, submit applications and for education purposes. While this is critical to the improvement of IT skills, it also requires that we educate customers about the associated benefits and risks of using technology to enable them to control their online experiences.

Ixion is committed to:

- **ensuring security measures are strong and reliable** – measures include enhanced internet filtering and firewalls to protect, servers and work stations and prevent accidental or malicious access of systems or information.
- **managing risks** – by conducting risk assessment on the use of any new technologies and external online platforms.
- **promoting safe and appropriate user behaviour** – Ixion will not tolerate abuse of IT systems. Incidents of bullying, harassment or unacceptable conduct will be treated seriously. Where conduct is found to be unacceptable, Ixion will deal with the matter internally. Where it is considered illegal, the matter will be reported to the police.
- **ensuring storage of information is secure and meets all legal requirements** – customer and staff information is stored by Ixion in line with our Information Assurance & Security Policy. Ixion staff will keep personal information safe and secure at all times, and only share this information with consent of the information owner or in line with the above policy.
- **educating staff and customers in e-safety** – we will support and educate our staff and customers to ensure they are able to recognise the risks and make informed judgements.
- **effectively managing any incidents which threaten e-safety** – through information security monitoring and clear reporting and investigating processes.

Definition

E-safety describes the process of limiting the risks to children, young people and vulnerable adults when using internet, digital and mobile technology. Risks include:

1. **Content**: exposure to age-inappropriate material, inaccurate or misleading information, or socially unacceptable material, such as that inciting violence, hate or intolerance; illegal material, such as images of child abuse.
2. **Contact**: grooming using communication technologies, bullying via websites, mobile phones or other forms of communication device.
3. **Commerce**: exposure to inappropriate commercial advertising, online gambling services or commercial and financial scams.

Communication

Staff will receive training in e-safety as part of their induction, and are required to familiarise themselves with all related policies and guidance available on the Ixion Cloud shared drive. Staff must ensure that customers are aware of who they can talk to should they have any e-safety concerns as part of their individual programme induction. Individual curriculum may have specific e-safety modules, but where this is not the case customers should receive an e-safety briefing before accessing the internet.

Staff, Learners and Customers -Staying Safe

It is impossible to be completely safe while using electronic communication, particularly the internet. Ixion staff, customers and learners may reduce the risks by following the steps below.

Search Engines

Search engines enable the rapid search of the Internet for information including text, images, video or audio content. Searching typically involves entering a word or words into a search box and clicking the search button to produce a list of relevant websites. The more accurate your search e.g. using a full phrase in "_" rather than singular words, the more relevant the search results will be and less likely that unwanted results will be returned. For example, if you are searching for information on the planet Mars, entering 'planet mars' as the search criteria will return more relevant results than just entering 'Mars'.

Take care to spell correctly when typing in a search. Even a small typing error can return unwanted results.

Remember that not all the information held on websites is reliable. Do not take any information on face value. For better assurance, you should try to ensure that you have visited a genuine authority for what you are searching. You can try to establish this by checking domain names in the address bar carefully with every page that you visit, you can also hover over links with the mouse pointer to check at the bottom of the browser the domain you will be visiting i.e. gov.uk domain in https://www.gov.uk/browse/driving

It is important to identify when search results are sponsored rather than normal search results. Sponsored results are "paid for advertising" so may not always provide relevant or accurate information. Even malicious content can be delivered for a short time though paid advertising before it is found which are normally the first few results in a search. You should always also hover over these links to check the domain before visiting as the title of an advert can be used to present a misleading website address. Google search engine now denotes adverts with an "Ad" logo prefix.

Downloads

Unless you are an IT or Data professional it is forbidden to deliberately download any filetypes that have the capabilities of making changes to a system. These are in the executable or script categories and include but are not exclusive to; .bat, .exe, .msi, .cmd, .ps1 and .js if downloaded rather than running in the background from a legitimate website. If you are seeing blocked messages from a staff computer then it is likely a forbidden filetype is attempting to run and you should contact the IT department.

Social Networking Sites

Please refer to the Social Media Policy for specific guidelines on company policy regarding the use of social media. Although some safety guidelines have been highlighted below as a rule employees should not 'post' to social networking sites with an Ixion email address without specific approval for a specific business case such as marketing. Personal use of social networking on company devices is strictly prohibited due to the possibility of an accidental information leak from a copy/paste mishap or similar.

Social networking sites (like Facebook, LinkedIn) are online 'communities' of internet users to share information. Members of the community create an online 'profile' to share their personal information. It is important that users look after their personal information properly to minimise the risk of cyber bullying, invasion of privacy, identity theft, grooming etc.

After seeking company approval, when using social networking sites:

- Don't publish personal information like location, email address, phone number or date of birth.
- Be very careful about what images and messages are posted, even among trusted friends – once they are online they can be shared widely and are extremely difficult to remove.
- Keep a record of anything abusive or offensive received and report any trouble to the site management (most sites have a simple reporting procedure, normally activated by clicking on a link on the page).
- Be aware that publishing or sharing anything which would mean breaking a copyright agreement is illegal.
- If you make an online friend and want to meet up with them in real life, take safety precautions such as going with a group of people, making sure friends and family know where you are, only meeting in a public place etc.
- consider creating separate 'professional' and 'personal' profiles with different security settings to ensure your personal profile is private.
- Think before posting any photos of yourself (or comments) - ask yourself if you would be comfortable with colleagues, managers or customers seeing them. Never upload photos in response to a request from someone you do not know and trust.

When using Twitter:

- Check who is following you regularly and block anyone you do not wish to see your "tweets".
- Set your privacy settings to limit who sees your updates.
- Change your user name so it is not your actual name.
- Check the settings to control what others can find out about you.
- Consider using a graphic or an icon rather than a photo of yourself in your profile. If you do use a photo, make sure it is not rude, 'suggestive' or would otherwise attract inappropriate contact.

E-mail

- Do not forward chain letters to anyone else, just delete them.
- Do not impersonate anyone else using e-mail.

- Do not use e-mail to send comments or information that is defamatory or libellous, or use e-mail as a means of harassment, intimidation, annoyance or bullying to anyone else. Only send messages that you would be happy to receive.
- Do not reply to pestering, offensive or suggestive e-mails, but report them to a line manager or adviser/tutor.
- Never give bank details or financial information in an email.

Cyberbullying

Cyberbullying is when someone bullies' others over the internet using Social Media or on a mobile phone by sending abusive emails or texts directly or by posting nasty comments or humiliating images for others to see.

Grooming and radicalisation can also take place using the internet's social media sites so please be vigilant when people are trying to befriend you, especially when they are asking to meet you or trying to encourage you to adopt beliefs or persuade you to join groups.

If you are worried or have any questions or concerns regards to this, then you should speak to your Assessor and Ixion safeguarding officer.

e-Safety Staff, Learner and Customer Concerns & Complaints

Ixion staff are responsible for ensuring the safety of customers and learners and should report any concerns to their Line Manager. Staff are required to familiarise themselves with the appropriate policies and guidance available through the Ixion intranet. Staff must ensure that customers and learners are aware of who they can talk to should they have any e-safety concerns.

All learners are responsible for using IT systems in accordance with guidance issued during the course/programme being undertaken. Learners using our online systems will be issued with their own login and password details and must be aware that postings to this site will be monitored.

All Work Programme and CWP customers are responsible for using the IT systems available to them in accordance with the guidance provided in centres.

Staff should raise any queries and concerns with their line manager in the first instance. Customers should raise issues with their adviser/tutor or local manager.

The manager will take action to investigate in line with Ixion's Safeguarding, Bullying & Harassment or Information Assurance Policy with assistance from the Head Service IT. Concerns relating to safeguarding, will be referred immediately to the Local Safeguarding Champion or Designated Safeguarding Manager.

Proven incidents of misuse of digital communication or unacceptable use will be dealt with through Ixion's disciplinary policies for staff and customers.

Associated Policies

This Policy and associated procedures should be read in conjunction with the following Policies:

- Information Assurance & Security
- Anti-Harassment & Bullying
- Data Protection
- Discipline & Dismissal
- Safeguarding
- Social Media

Responsibilities

- **Head of Service IT:** responsible for ensuring staff development and training is provided on e-Safety; recording, investigating and resolving incidents; ensuring system safeguards are fully implemented; promoting e-Safety across all areas of the business.
- **All staff**: responsible for using IT systems and mobile devices in accordance with Ixion IT polices; ensuring all digital communications with customers is professional at all times and in line with our email usage policy; ensuring the safety of customers and reporting any concerns to their Line Manager.
- **Learners and Customers**: responsible for using IT systems in accordance with guidance issued during the course/programme being undertaken. Learners using Ixion's e-portfolio system will be issued with their own login and password details and must be aware that postings to this site will be monitored.

Monitoring & Review

The Head of Service IT will monitor the effectiveness of this policy by reviewing incident reports and gaining feedback from staff and customers as part of our standard information assurance and security auditing.

This policy will be reviewed annually to ensure it continues to adapt and respond to changing technology usage and development, legislative requirements, emerging best practice, and continues to be effective and relevant to the wider business. The Head of Service IT will report back to the Board on the performance of the policy with recommendations for improvement if required.