Comprehensive plans are in place to improve our institutional cyber security

All staff, students and visitors understand they are responsible for cyber security

CYBER SECURITY

Cyber Hygiene 1
Year 1 – all staff and students trained

- Clear processes are in place for reporting security incidents as quickly as possible.
- IT staff categorise and handle cyber security events efficiently and effectively.
- Roles and responsibilities are defined and understood at all levels in the organisation.

You'll know what to do

- General cyber security training has been provided to all staff and students which is available 24/7.
- Online guidance and trained support services have been provided and are available 24/7.

You'll know how to get help

- Training is planned to up-skill all staff, students and visitors to optimise our front-line defences against cyber-attacks.
- Senior managers understand the threat landscape and risk management is in place at central and departmental levels.
- ISD staff and faculty IT colleagues routinely monitor cyber security events in order to inform best practice.

You'll know it's taken care of

Cyber Resilience 2
Year 2 – security dependent income opportunities optimised

- Cyber security accreditation is in place, enabling Strathclyde to optimise security dependent income opportunities.
- Anti-virus and OS updates are delivered automatically.
- Secure identification and management processes are in place for bring-your-own-devices (BYOD).
- Data is accessible from any location once a device has been authenticated.

You'll know what to do

- All staff, students and visitors understand they are responsible for cyber security.
- Specialised role-related training is in place and supports career progression where sensible.
- Training requirements are embedded into the induction processes for all staff and students.

You'll know how to get help

- Different types of simulation tests have been evaluated and useful ones have been adopted.
- Escalation processes for major cyber security incidents are streamlined and effective.

You'll know it's taken care of

Cyber by Design 3
Year 3 – embedded into business as usual

- Desktop maintenance and software installation is automated.
- Role-based authentication means users can access their desktop profile whenever, wherever, and from whatever device they are using.
- Multi-factor authentication is used for important secure actions, like changing your password.
- Cyber security standards are built into all new infrastructure and software development.

You'll know what to do

- Training and online materials are routinely reviewed to ensure they are kept up-to-date and relevant.
- Ad hoc specialist campaigns are used to promote awareness when new security threats emerge.
- Cyber security messages are consistent across all departments and media.

You'll know how to get help

- Processes are reviewed by routine and incorporate lessons learnt from internal and external incidents.
- Customers Services feedback is in place to identify where support processes could be improved.

Comprehensive plans are in place to improve our institutional cyber security

All staff, students and visitors understand they are responsible for cyber security

- General cyber security training has been provided to all staff and students which is available 24/7.
- Online guidance and trained support services have been provided and are available 24/7.
- Lightweight awareness and training has been provided for visitors and 3rd parties.
- ISD Cyber Security Team disseminate ad hoc messages relating to end-user cyber security practice.

- Senior managers understand the threat landscape and risk management is in place at central and departmental levels.
- All IT staff understand the threat landscape and routinely contribute to risk assessments and management.
- Comprehensive plans are in place to up-skill all staff, students and visitors to optimise our front-line defences against cyber-attacks.
- ISD staff work with faculty IT colleagues to routinely monitor cyber security events, both internally and externally, in order to inform best practice.
- Comprehensive plans are in place to improve our institutional cyber security.

- Clear processes are in place for reporting security incidents (and/or events?) as quickly as possible.
- IT staff categorise and handle cyber security events efficiently and effectively.
- Escalation processes for major cyber security incidents are in place and documented.
- Roles and responsibilities are defined and understood at all levels in the organisation.

You'll know it's taken care of

You'll know what to do

You'll know how to get help

1

Cyber Hygiene

Year 1 – all staff and students trained

Comprehensive plans are in place to improve our institutional cyber security

All staff, students and visitors understand they are responsible for cyber security

- All staff, students and visitors understand they are responsible for cyber security.
- Specialised role-related training is in place and supports career progression where sensible.
- Training requirements are understood and driven by policy.
- Training requirements are embedded into the induction processes for all staff and students.
- Training materials and online guidance have been optimised to reflect feedback from Year 1.

- Cyber security accreditation is in place, enabling Strathclyde to optimise security dependent income opportunities.
- Secure identification and management processes are in place for bring-your-own-devices (BYOD).
- Data is accessible from any location once a device has been authenticated.
- Anti-virus and OS updates are delivered automatically.
- Apps are installed automatically from a single catalogue.
- Management information drawn from the app catalogue is used to define role-based standard build profiles and optimise software license costs.
- Robust processes are in place to support changes in role ensuring that end-users can access data when, where and for the duration they need to as quickly as possible.
- Processes for desktop management have been reviewed and consolidated to achieve standardisation where sensible.

- Different types of simulation tests have been evaluated anduseful ones have been adopted.
- Escalation proces ses for major cyber security incidents are efficient and effective.
- Processes are in place for raising awareness of lessons to be learnt from breaches reported in the news.

You'll know it's taken care of

You'll know what to do

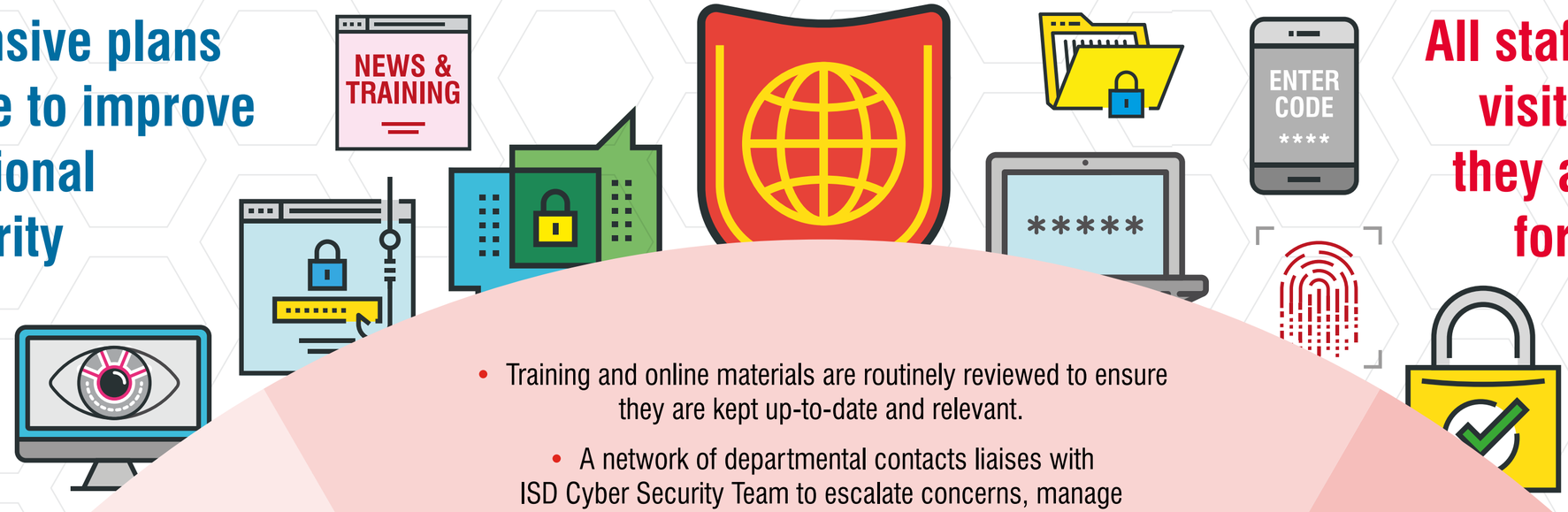
You'll know how to get help

2

Cyber Resilience

Year 2 – security dependent income opportunities optimised

Comprehensive plans are in place to improve our institutional cyber security



All staff, students and visitors understand they are responsible for cyber security

- Training and online materials are routinely reviewed to ensure they are kept up-to-date and relevant.
- A network of departmental contacts liaises with ISD Cyber Security Team to escalate concerns, manage training and disseminate key information updates about cyber security practice.
- Ad hoc specialist campaigns are used to promoteawareness when new security threats emerge.
- Refresher training requirements are understood and driven by policy.
- Cyber security messages are consistent across all departments and media.

- Desktop maintenance and software installation is automated so admin rights have been restricted to user accounts with specialist requirements (VIP).
- Devices are a portal to access and work with data – not the place where data is stored.
- Role-based standard build profiles that automatically deliver user-related software and services are in place.
- Role-based authentication is in place so that end-users can access their standard build profile whenever, wherever, and from whatever device they log into.
- Multi-factor authentication is in place for important secure actions, like changing your password.
- Agreed cyber security standards are built into all new infrastructure and software development.
- The threat landscape is routinely reviewed and the risk management of emerging issues is built into the University planning round.

- Processes are reviewed by routine and incorporate lessons learnt from internal and external incidents.
- Customers Services feedback is in place to identify where support processes could be improved.

You'll know it's taken care of

You'll know what to do

You'll know how to get help

3

Cyber by Design

Year 3 – embedded into business as usual