The Langstane Group

Information Security Policy

Date approved by leadership team	11 September 2024
Board of Management	Board of Management
Approval date	14 November 2024
Implementation date	November 2024
Review date	November 2027
Version	V4

Version	**Date approved**	**Changes**
Version 1	2019	First issue
Version 2	16/03/2020	Section on independent databases and the intranet added, general strengthening of guidance relating to security of data
Version 3	12/11/2021	Added a subsection on default passwords, this is a stipulation of the Cyber Essentials checklist.
Version 4	30/07/2024	Updated policy document to include audit recommendations and current standards.

1. Introduction

Langstane Housing Association is a Co-operative and Community Benefit Society, and a registered social landlord with charitable status.

The Langstane Group (Langstane / the Group) consists of Langstane Housing Association Limited and its wholly owned subsidiaries.

This policy applies to all entities of the Langstane Group.

Langstane has a legitimate need to collect, store and use certain types of information about its staff, residents, customers and others associated with the Group in order to carry out its functions. Therefore the management and use of such information, whether in manual or electronic format, will be to the highest standards possible whilst remaining proportionate to the risks present and meeting the requirements of the General Data Protection Regulations (GDPR).

This policy applies to all system users of information held in the Langstane Group's IT facilities and assets owned / leased by Langstane or to devices that connect to a Langstane network or reside at a Langstane site. It also covers all information that is held manually for, by, or on behalf of, the Langstane Group.

The term 'system user' includes, but is not limited to, all employees, contractors, consultants, temporary and other paid or voluntary workers at, or on behalf of, the Langstane Group. All personnel affiliated with third party organisations providing services to and / or processing information on behalf of the Group must adhere to this policy or provide their company's policy that will be approved by the Group's IT service in advance.

2. Aim of the policy

The aim of this policy is to ensure:

2.1 Information provided to and held by the Group remains accurate, up-to-date, and free from corruption;

2.2 Information is held confidentially and protected against unauthorised access at all times. This includes access to Group systems and networks;

2.3 System users are aware of their responsibility for the security of data and use of systems under their control; and

2.4 System users are aware of the escalation processes in place and what to do in the event of discovering a breach or potential breach of security including suspected malware or virus infection of any device.

3. Objectives

Information Security controls are designed to protect members of The Group and The Group's reputation through the preservation of CIA (Confidentiality, Integrity and Availability).

- Confidentiality - knowing that key data and information can be accessed only by those authorised to do so.

- Integrity - knowing that key data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version.

- Availability - knowing that the key data and information can always be accessed.

This Policy ensures the integrity of its electronic devices and systems is maintained and employees are aware of their responsibilities to maintain the security of devices and systems at all times.

Langstane provides employees and others with access to information in other formats including verbal and written information. It is the role of everyone involved with the Group to understand and comply with this policy when handling and / or using data provided to / by, the Group.

4. Links to other strategic documents and policies

The Group's Information Security Policy is linked to a number of strategic documents and policies in particular but not solely:

- Privacy Policy;
- IT Strategy;
- IT Disaster Recovery Plan;
- Risk Management Policy;
- Staff Handbook;
- Codes of Conduct.

5. Policy

The Langstane Group operates on a cloud architecture with system user access enabled through a number of routes such as Desktop, Laptops, Tablets and Mobile devices, the group also holds data on vendor 'software as a service' based solutions which are hosted independently by the vendor.

All devices have the ability to communicate internally with each other and externally to customers and other businesses.

The Group's IT service holds a centralised register of all electronic / portable assets and systems used by or operated by the Group and monitors activity to identify any malicious or unusual activity. Although the majority of data is held electronically and can be accessed through electronic / portable devices, a significant amount of sensitive and / or confidential information is held manually and comes under the remit of this policy.

All information collated for or used by / on behalf of the Group belongs to the Group.

Information may only be accessed and shared to the extent it is authorised to do so and necessary to fulfil assigned roles and duties.

At no time will the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations, be violated.

An IT Disaster Recovery Plan is in place to deal with major incidents of electronic data loss / restricted access. This does not negate the responsibilities held by system users to ensure information security at all times.

Access to all information systems and use of electronic / portable devices is continually monitored to ensure compliance with policy and information security is maintained.

Inappropriate use or sharing of information will be dealt with robustly and appropriate action taken where a system user has deliberately or negligently used information inappropriately, or allowed information to be used by others who are unauthorised to access such information. This includes but is not limited to disciplinary action and / or involving external agencies such as the Police.

System users will ensure that when using Langstane Group devices or systems the following are followed:

6. Physical security

a. All electronic / portable devices are asset tagged and details held in an asset register;

b. It is the responsibility of anyone assigned a Langstane Group electronic / portable device to ensure they take reasonable care to preserve the physical security of the equipment under their control. This involves taking care to ensure liquids are not spilled on the equipment or material damage caused through misuse;

c. Devices may only be removed from their normal location with authorisation of service managers. Any loss or theft of a device must be immediately (within one working hour of being aware) reported to the IT service;

d. A screen lock is used when the device is unattended to minimise issues or the possibility of deliberate misuse by another person(s). Complex passwords are used to minimise the possibility of unlawful use;

e. Every care is taken to avoid theft, loss or unlawful / unauthorised use of any device, for example by leaving a device in an unlocked vehicle, or ensuring visitors to the Group are escorted to meeting rooms. Where employees / representatives from external organisations are working freely within the building (e.g. carrying out an audit, repairing equipment) they sign in and out when entering and leaving the building. A visitor pass is carried at all times and access restricted to areas legitimately required for the purposes of their visit;

f. System users have a responsibility to only view information they have a legitimate requirement to access to undertake their role. Where practical, information is restricted to 'system user groups' and permissions controlled centrally. Periodic checks are carried out to ensure access is still required, especially in relation to information of a highly sensitive / confidential nature;

g. All corporate owned devices will use multifactor authentication to access business resources wherever possible, suitable endpoint protection software must be used to reduce any possibility of introducing malware;

h. Where feasible, as much sensitive / confidential information as possible will be removed / redacted prior to a document / data being sent. Following checks to ensure sensitive information is required, and prior to sending information via email, care is taken to ensure the right recipient is chosen and the information is protected (e.g. by password protecting the information);

i. Whilst it is accepted that personal devices may be used to send work related information to Group email accounts (e.g. work related photos), personal email accounts are not used to conduct business on behalf of the Langstane Group;

j. When processing credit / debit card payments, the Group utilises the services of an organisation that is PCI DSS compliant;

k. Manual records that contain sensitive / personal information are securely stored at all times. When system users remove documentation that contains sensitive / personal information, care is taken to protect this from unauthorised access or loss or theft (e.g. it is not left in an area that can be viewed / removed by others including members of the public);

l. No member of staff will inappropriately participate in dialogue / post information that:

   i. Could identify an individual(s) to third parties through their association with the Group; and / or
   ii. Is private and confidential / sensitive / derogatory information about the Group.
   iii. This includes any posts made by individuals to social networks in their own name;

m. At all times, when a data cleansing exercise is being undertaken in keeping with the document retention schedule, manual and electronic records are destroyed securely;

n. Unused and legacy software and applications are removed from devices to reduce potential vulnerabilities;

o. Access to networks and systems is cancelled immediately upon receiving notification from the HR team and there maybe individual circumstances where this is also done for example if an employee; is suspended, is absent for long periods (to be determined on a case by case basis) or a contract ends;

p. All business data should be held digitally, if digital storage means are not possible then the data is to be held in an appropriate fire retardant filing cabinet. Business critical information is also held off-site by members of the senior management team in hard copy. This is accessible in an emergency;

7. Protection

a. All devices used by an employee, or access to a Group network, use complex password requirements to avoid inappropriate access to the device and to the

Langstane Group network. System users ensure passwords are a minimum of 10 characters long, use number(s), special character(s) and upper and lower case letters. All mobile and tablet devices will use pin protection;

b. Passwords used for work related devices and / or networks do not replicate those used for personal social media or other personal sites / services (e.g. Facebook). This improves the protection of work related systems. The same password is not used across all work related devices / sites;

c. System users ensure their network and other related passwords are not revealed to any other individual, including work colleagues. This includes family and other household members where a system user has access to home / mobile / remote working. Revealing the password to others or allowing others use of systems through the system user's account are expressly prohibited;

d. The use of a password manager or other similar password protection is encouraged. Information regarding password protection is provided by the Group's IT service;

e. All administrator access will be facilitated using a separate account with elevated privileges and will only be used for this purpose;

f. Where access to a website is only permitted through one log-in that is legitimately shared internally, the password used is unique and not replicated or similar to those used elsewhere by the member of staff setting up the password. A record of those with access to the password is held centrally in a password manager;

g. The passwords for password protected files are held securely in a central location to ensure they can legitimately be accessed in the future should the system user leave the Group;

h. All devices are secured with a password-protected screensaver with an automatic activation feature set to 30 minutes. System users lock the screen or log off when a device is left unattended;

i. On receipt of any new hardware or application all default passwords are immediately changed to maximise our businesses security posture;

j. Multifactor authentication will be enabled by default for all employees and all business applications which have the ability to utilise multifactor authentication controls;

k. Single-sign-on will be used where appropriate to minimise the need to have multiple sets of login credentials for applications and services;

8. Mobile working

a. Langstane recognises the advantages to both the Group and employees of mobile working, Devices provided to employees can be used both in the office or remotely. Under no circumstances will non-authorised devices or similar technology be permitted for use on the Langstane Group network;

b. System users are not permitted to divert Langstane information to personal devices without the express permission of the IT service. This includes, but is not limited to, emails and / or phone calls;

9. Remote access

a. Remote access to the network is desirable in certain circumstances to maintain operational efficiency. In many cases remote access originates from networks that may already be compromised or at a lower security position than the Langstane Group network. While these networks are beyond the Langstane Group's control, every step is taken to mitigate risks arising from these networks;

b. Access to the Langstane Group network is only available via the Langstane Group "Firewall appliances" and by no other means. Any system user given access through the "Firewall", whether employee, contractor, consultant or any other system user, ensures, as far as they are able, the network from which they are connecting is secure;

c. If the Langstane Group "Firewall" security software detects any risks from an attempted connection, access is denied. System users ensure that while connected to the Langstane Group network, the remote device is not connected to any other network, with the exception of personal networks that are under the complete control of the system user;

d. It is the system user's responsibility to ensure no non-authorised system user is able to gain access to, or use any of the features of the system. System users ensure their log-in details are kept secure at all items to prevent unauthorised access;

e. No unauthorised or personal storage or mobile devices will be connected to the Group's networks or systems. No copies will be made of restricted Group information without permission. No restricted Group information will be sent to a personal email account for printing or other use without permission;

10. Wireless access

a. Wireless access to the Langstane Group network is permitted to devices fitted with this capability and supplied to system users by the Langstane Group;

b. Wireless access is only be made via secure networks and never made using public Wi-Fi access points unless pre authorised by the Group's IT service. This will be permitted in limited situations only and where the level of monitoring against attack is deemed to be appropriate e.g. within local authority meeting rooms. In situations where there is no suitable access point, mobile devices may be connected to the system using 3G or 4G through the device provider;

11. Data storage

a. The Langstane Group stores information on its main infrastructure within various data servers which are held in the cloud. These all have security controls in place allowing access as required to conduct legitimate business activities;

b. Data is not stored on hand held or portable devices as far as practical and appropriate. In circumstances where data is required to be held on such devices it is uploaded to the system network as soon as practical and purged from the mobile device;

c. Where it is necessary to transfer sensitive / personal / confidential data to a third party and this cannot be done electronically through the network or via a secure file transfer facility, such data will be downloaded onto an encrypted and password protected USB stick which will be available from the Langstane Group IT service. No confidential company / personal data will be stored on an unencrypted USB or similar device under any circumstances;

d. Prior to disposal of any corporate owned devices the device and any associated memory cards are returned to the Group IT service for secure data destruction and/or obfuscation;

e. Manual records that contain sensitive / personal information are securely stored at all times. When system users remove documentation that contains sensitive / personal information, care is taken to protect this from unauthorised access or loss or theft (e.g. it is not left in an area that can be viewed / removed by members of the public);

f. Access to critical systems and key data and information will only be granted on a need to know basis. Segregation of duties will be implemented where applicable and role based access controls are also in place to prevent unauthorised access to data;

12. Data backups

a. Information held electronically by the Group is backed up appropriately through a cloud based configuration and a robust data back-up strategy is in place to protect the Group against potential security incidents such as but not limited to malware attacks, ransomware attacks;

b. Data backups will be monitored daily (weekdays only) by the IT team and the backup schedules must be documented and regularly reviewed;

c. The IT team are responsible for regularly checking the data backup tasks and must ensure that adequate backup and system recovery practices, processes and procedures are followed by the vendor;

d. Backup and recovery testing must be performed annually to ensure the process is functioning correctly;

e. Any request to restore data from backups must be approved by the department manager and/or director and must be logged within the IT portal;

13. Data retention

a. The Group operates a document retention schedule. This details the timescales for the retention of data in both electronic and manual format. There are control systems in place to ensure the document retention schedule is adhered to;

14. Phishing and related attack vectors

a. The Group is not isolated from random, but increasing, attempts to access its networks and systems. This can be in the form of spam, phishing and other scam emails and can also be from the download or viewing of attachments from unsecure locations (e.g. menus for events);

b. Regular maintenance is undertaken to ensure devices and systems run smoothly and to fix any identified or possible vulnerabilities;

c. Firewalls and endpoint protection is used at all times by the Group and software updated to avoid infection. The installation of such is centrally controlled by the Group's IT service;

d. Extreme caution is used when opening attachments, 'safe attachments' is used as part of the groups IT security offering which scans contents and attachments to ensure no viable threats are identified;

e. No bulk (spam) emails will be forwarded to others through Group network, IT endpoint policies will be in place to restrict bulk emails;

f. Security checks are carried out prior to engagement with people pertaining to be tenants or other customers. This includes, but is not limited to, those who wish to gain personal information regarding a tenant or those who wish the Group to change the payment methods for contracts in place;

g. Training is provided to ensure information included in publicly available documents, including those posted online, is appropriate and reduces the risks to the group of attack;

15. Accuracy of data

a. Regular checks are made to ensure the data held is up-to-date and accurate;

b. Archived data is held securely but separately (where practical to do so) to avoid unauthorised access;

c. Information relating to former employees / customers is cleansed in keeping with the Group's documentation retention schedule;

16. Misuse of assets

a. The Group has a responsibility to ensure its assets are used for legitimate business purposes therefore it monitors for any inappropriate activity;

b. Inappropriate activity will be dealt with robustly and may involve notifying appropriate statutory organisations e.g. the Police;

17. Email usage

a. Langstane Group email accounts are for business related purposes only. Limited personal communication is permitted but non-Langstane related commercial uses are strictly prohibited;

b. Emails are only retained if they qualify as a legitimate business record and on-going business reasons are in place to preserve the information;

c. Without exception, the Group's email system is not to be used for the creation or distribution of offensive, derogatory, religious, political or otherwise inappropriate messages as defined by the senior management of the Langstane Group, including those against other system users due to a protected characteristic(s) regardless of whether or not the intention is to cause offence. System users who receive emails of this nature will report these to their line manager as a matter of urgency;

d. Third party email systems will not be used to conduct business, create or memorialise any binding transactions, or to store or retain information on behalf of the Group;

e. The creation, viewing and distribution of chain emails and those of a humorous / pyramid nature is prohibited;

f. System users have no expectation of privacy in anything they store, send or receive on the Group's email system;

g. Messages (inward and outward) may be monitored without prior notice and may form part of a disciplinary process. The Group is not obliged to monitor email messages;

h. The Group's documentation retention schedule determines the length of time emails are kept;

18. Access to independent databases and applications

a. Access to Group data held within independent databases and applications that are not linked to the Group's network is subject to the same level of requirements as that of data held on the Group's network and therefore must not be accessed / shared inappropriately, must be kept up-to-date and must be disposed securely;

b. The information held remains in the ownership of the Group and access will be tightly controlled;

19. Intranet

a. The Group’s intranet facilities are a work related resource and is the main location of up-to-date corporate documentation in the form of business plans, strategies, policies, procedures and forms;

b. Without exception, the Group’s intranet is not be used for the creation or distribution of offensive, derogatory, religious, political or otherwise inappropriate messages as defined by the senior management of the Langstane Group, including posts against other system users due to a protected characteristic(s), whether or not the intention is to cause offence. Any post of the above nature will be reported to a line manager as a matter of urgency;

20. IT Assets; security, remediation and responsibilities

a. IT Assets will have encryption in place wherever feasible;

b. All IT assets will have a mobile device management platform installed to manage and protect the endpoints;

c. All IT assets (both physical and virtual) will have automated application and software patching in place, all vulnerabilities with a score of critical or high will be patched as soon as practicable;

d. IT assets will be monitored to ensure compliance to business policies and to ensure the devices and our employees are protected;

e. All employee IT assets including but not limited to mobiles, tablets and laptops, should always be switched on during working hours, or when on-call, except where it would be inappropriate for the device to ring e.g. in meetings, whilst driving etc;

f. Where patching is not automated, the IT service will instruct employees when and how to apply manual patching for all devices and applications;

g. Employees are required to apply any security updates to there business assets as soon as there notified either by the IT team or the asset itself;

h. Where patching or updating a device is not possible this will be logged in our operational risk register, from which the risk will be managed;

i. Annually an independent penetration test will be performed to ensure the business has the correct control measures in place and to ensure that the business is in compliance with industry best practices such as ‘cyber essentials’;

j. All endpoints will have endpoint protection services installed such as anti-virus, content filtering and endpoint firewall protection to protect the asset and the employee;

k. Multifactor authentication will be used wherever possible and in conjunction with single-sign-on capabilities if possible;

l. Sensitive and person identifiable information must never be sent by text message as it is not a secure method of communication;

m. For mobile phones and tablets only applications from the Langstane google managed play store are allowed, users are also prohibited from removing applications from there business devices without consent from the IT team;

21. Firewalls

a) Firewalls will be deployed at all network entry access points both virtually and physically;

b) All business firewalls will be configured to only allow access through ports where business justification is given, a record of this will be kept by the IT service;

c) Default deny-all-rule is in place on all firewalls that will prohibit all inbound and outbound traffic unless explicitly allowed, firewalls rules will be reviewed regularly to ensure there current;

d) Content filtering is applied on all endpoint devices, below are the categories currently being blocked;

Categories

- Cults
- Gambling
- Nudity
- Pornography/Sexually Explicit
- Sex Education
- Tasteless
- Violence
- Child Abuse Images
- Criminal Activity
- Hacking
- Hate & Intolerance
- Illegal Drug
- Illegal Software
- School Cheating
- Self-Harm
- Weapons
- Games

e) Firewalls will be regularly monitored and updated, firewall logging will also be in place on all permitted traffic so that suspicious activities and anomalies can be identified;

f) If remote access is required then Virtual private network connectivity will be in place to ensure only authorised individuals can access the network through the firewall;

g) The IT service in conjunction with our support partner will regularly conduct compliance checks to ensure that firewall configurations adhere to industry standards and regulatory requirements;

22. Roles and responsibilities

Board of Management and Chief Executive

Overall responsibility for information security lies with the Board of Management with day to day implementation and adherence delegated to the Chief Executive.

Departmental Directors

Departmental Directors have responsibility for identifying, recording and reviewing information held by their department in paper and electronic format. They hold responsibility for determining permission levels and ensuring staff are aware of the requirements for information security.

Managers

All managers have a responsibility to ensure strict adherence to policy in all aspects of information security and for highlighting any potential issues they may witness that has the potential to expose the Group to greater risk.

The Group's IT Manager is responsible for guidance regarding any aspect of information security regarding electronic / portable devices and the Group's networks and systems. The Group's IT Manager is responsible for ensuring Cyber Essentials accreditation is obtained and maintained and an up-to-date IT Disaster Recovery Plan is in place at all times.

The Group's leadership team is responsible for providing guidance on all aspects of data protection in conjunction with the IT Manager. Both the management and leadership teams are responsible for recording and reporting each reported incident for their area of responsibility.

All system users

Every system user has a responsibility to maintain the security of Langstane Group information by taking a proactive stance rather than a reactive one.

As part of the Group's staff and Board of Management induction process and on-going training programme, awareness of information security is highlighted and refreshed on a regular basis. The procurement process is used to identify the requirements for contractors and others employed by the Group to adhere to this policy and play an active role in contributing to the Group's information security.

If a system user suspects an attempt to access or use information relating to the Group and / or its customers is fraudulent or otherwise inappropriate, this will be reported to the Group's IT service immediately.

Lost or stolen devices are deactivated by the Group’s IT service immediately (within one working hour) following notification. System users are required to notify the IT service as soon as possible following discovery of the lost / stolen device (within one working hour of becoming aware of the lost / stolen device).
Where an individual suspects someone is accessing / has accessed / or has attempted to access information that is outwith their remit and responsibilities, they will advise their immediate line manager as soon as practical. If their line manager is the person suspected of sourcing information inappropriately, a more senior member of staff will be advised.

Where a breach has occurred and sensitive / personal / confidential information has been divulged, the Data Controller (Chief Executive) and the central point of contact for Data Protection matters (Director of Housing) will be advised immediately. If appropriate the Information Commissioner’ Office will be advised.

Visitors to the Group are escorted by a member of staff when entering staff areas as they may be exposed to data that is of a confidential, sensitive or private nature. An exception is made when visitors are working within the office (for example to carry out an audit or repair a piece of equipment). In this situation, the visitor will sign in and out of the building and others be advised of their presence and take appropriate action to ensure information is secure.

23. Monitoring and review

Periodic monitoring will be instructed by departmental Directors to ensure within their areas of responsibility, access to information and information security is in keeping with agreed policy.

Independent internal audit of information security will be carried out at least once every five years. Where issues are found, monitoring will be increased in keeping with the severity of the breach.

Breaches of data protection are reported to the Board of Management on an annual basis or immediately if a notifiable / significant event.

This policy will be reviewed every three years following the date of implementation or where a change in legislation or regulatory framework is implemented and it is deemed appropriate to review the policy sooner.

In the event the policy is not reviewed within the above timescale, the latest approved policy will continue to apply.

24. Equality and diversity

The Langstane Group is committed to promoting equality and diversity across all areas of work. Discrimination or harassment of any kind is not tolerated.

If you would like this document in large print, please contact Support Services on 01224 423000.

Appendix 1

Further information

Get Safe Online (www.getsafeonline.org). A joint initiative between the government, law enforcement, leading businesses and the public sector to provide computer users and small businesses with free, independent, user-friendly advice that will allow them to use the internet Cyber Street.

Cyber Street (www.cyberstreetwise.com) is a cross-government campaign, funded by the National Cyber Security Programme, and delivered in partnership with the private and voluntary sectors. The campaign is led by the Home Office, working closely with the Department for Business, Innovation and Skills and the Cabinet Office.

The National Cyber Security Centre (https://www.ncsc.gov.uk/) was set up to help protect critical services from cyber attacks, manage major incidents, and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organisations.

Cyber Essentials (www.gov.uk/government/ publications/cyber-essentials-scheme-overview). The Cyber Essentials scheme provides businesses small and large with clarity on good basic cyber security practice. By focusing on basic cyber hygiene, your company will be better protected from the most common cyber threats. Cyber Essentials is mandatory for central government contracts advertised after 1 October 2014 that involves handling personal information and providing certain ICT products and services. It has been developed as part of the UK's National Cyber Security Programme in close consultation with industry.

10 Steps to Cyber Security (https://www.gov.uk/ government/publications/cyber-risk-management-aboard-level-responsibility). The 10 Steps define and communicate an Information Risk Management Regime which can provide protection against cyber attacks.

Action Fraud (https://www.actionfraud.police.uk) is the UK's national reporting centre for victims of fraud or financially motivated internet crime. Action Fraud records and refers these crimes to the police and provides victims with a crime reference number, support and advice.

Appendix 2

Legislation and regulations relevant to information security

The following legislation covers information security:

General Data Protection Regulation (EU) 206/679 and associated law (known as GDPR)
Superseding the Data Protection Act 1998 and other data protection regulations, GDPR is European Union legislation that came into effect on 25th May 2018.

Counter-Terrorism and Security Act 2015
Accessing websites or other material which promotes terrorism or violent extremism or which seeks to radicalise individual to these causes constitutes an offence under this Act.

Defamation Act 2013
The Defamation Act 2013 was introduced in order to reform the law surrounding defamation and to ensure that a fair balance between the protection of reputations and freedom of expression was being attained.

Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011
This Amendment obliges websites to inform users about their use of cookies and seek consent for setting more privacy intrusive cookies.

Equality Act 2010
This Act legally protects people from discrimination in the workplace and in wider society. It replaced previous anti-discrimination laws with a single **Act**, making the law easier to understand and strengthening protection in some situations.

Digital Economy Act 2010
This Act regulates the use of digital media in the UK.

Terrorism Act 2006
This creates a number of offences and under Section 19, imposes a duty on organisation to disclose information to the security forces.

Police and Justice Act 2006
Section 39 and Schedule 11 of this Act amends the Protections of Children Act 1978 to provide a mechanism to allow police to forfeit indecent images.

Fraud Act 2006
Section 10 (1) is the only section to cover Scotland and this amends the Companies Act 1985 extending the maximum custodial sentence permissible for fraudulent activities.

Freedom of Information Act 2000
Although not yet enacted for housing associations, it is expected this will happen in early 2020.

Regulation of Investigatory Powers Act (RIPA) 2000
RIPA regulates the powers of public bodies to carry out surveillance and investigation and also deals with interception of communications.

Human Rights Act 1998
This sets out, in relation to privacy, a right to respect for an individual's "private and family life, his home and his correspondence", a right that was embedded in the data protection legislation (now superseded by GDPR).

Computer Misuse Act 1990
This Act was intended to deter criminal s from using a computer to assist in a criminal offence or from impairing or hindering access to data stored in a computer.

Official Secrets Act 1989
This Act provides the main legal protection in the UK against espionage and the unauthorised disclosure of information.

Copyright, Designs and Patents Act 1988
This defines and regulates copyright law in the UK and categorises different types of works that are protected by copyright.

Malicious Communications Act 1988
This Act makes it illegal to "send or deliver letters or other articles for the purposes of causing stress or anxiety".

Limitation Act 1980
The Limitation Act 1980 enforces time limits within which a party must bring a claim, or give notice of a claim to the other party. They are enacted by statute, predominantly the Limitation Act 1980

Appendix 3

System User Agreement

All system users must read and sign they agree to the terms and conditions set out in the information security policy and this system user agreement.

a) All access to networked IT systems is via individual username and password with multifactor authentication in place. System users must never access networked systems using a computer that is logged on by another system user, nor must they enter another system user's details to attempt to gain access, or must they divulge their own password to enable another system user to access networked systems. When not in use, system users must either log off or lock access to their workstation if they leave the office;

b) All IT systems are provided for the sole purpose of conducting the Langstane Group's work or related activities. Under certain circumstances and with prior approval of the senior management team, private use may be used where:
- such activity is undertaken in the system user's own time and is not excessive
- such activity does not undermine the operational capability of the Langstane Group or its IT systems
- providing such activity is legal, ethical and does not contravene any Langstane Group policy or is detrimental to its image;

c) System users must not import data onto Langstane Group systems via removable media or the internet without prior approval of their line manager or the IT manager;

d) System users must not install software onto the system under any circumstances. Requests for installations will be made via the IT service;

e) System users must not reconfigure systems or applications software other than in a manner for which they have authority and have been trained to do so. System users may make appropriate changes to their user profile such as colour scheme and desktop layout;

f) System users must avoid contact with any cabling at the rear of all IT equipment;

g) System users are advised to be aware of poor posture when using IT equipment and to take regular breaks away from their visual display units (five minutes every hour is recommended);

h) System users with access to Langstane email facilities should check their email at least twice every working day. When away from the office for more than five working hours, an appropriate 'out of office' message will be set giving a date / time for return;

i) Use of email is for Langstane work-related activities and very limited private use only. All email content must be above reproach and must not contain any material that could contravene other corporate policies, cause harassment to recipients, or be illegal. Care must be taken when transmitting data as email is insecure;

j) Internet access is limited to work-related activities and limited private. Access for private use may be withdrawn at any time without prior notice. Access to, or downloading inappropriate material such as pornography or racist material, will be treated as gross misconduct;

k) All system users must be aware their activities on the network are monitored and leave an audit trail. If there is reason to believe any Langstane Group policies have been breached, this audit trail may be used to gather evidence of inappropriate use. Any such breaches will be dealt with through the disciplinary procedures;

l) Any activity that breaches UK, European or International law (e.g. viewing inappropriate images, computer hacking) will be reported to the relevant authority and may lead to further action being taken, this includes legal action.

I agree to abide by the terms and conditions of the Information Security Policy and the terms and conditions of this system user agreement.

Signed ………………………………………………………… Date ……………………………

Name (please print) ……………………………………………………………………………………